Anno 2 - N. 16
2 Gennaio/16 Gennaio 2003

Boss: theguilty@hackerjournal.it

Editor: grAnd@hackerjournal.it,

Graphic designer: Karin Harrop

Contributors: aDm, Bismark.it, Enzo Borri, CAT4R4TTA, Roberto "decOder" Enea, Khamul, Lele-Altos.tk, {RoSwEiL}, Paola Tigrino

Publishing company
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing
Stige (Torino)

Distributore
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81-
Tel. 06.33455.1 r.a.
20134 Milano, via Cavriana, 14
Tel. 02.75417.1 r.a.
Pubblicazione quattordicinale registrata al Tribunale di Milano il 25/03/02 con il numero 190.
Direttore responsabile Luca Sprea

HJ: INTASATE LE NOSTRE CASELLE

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati.

redazione@hackerjournal.it

hack·er (hãk'∂r)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

***E** così Hacker Journal ha visto finire il 2002, e si appresta come tutti a iniziare questo 2003. OK, è vero. Non è da un anno intero che esiste HJ: chi ci segue dall'inizio, ha avuto in mano il primo numero lo scorso maggio. Da allora sono passati otto mesi. In così tanto tempo quasi ci si fa un bambino. Siccome l'inizio di un nuovo anno spinge la gente a fare bilanci del passato e propositi per il futuro, non ci sottraiamo a questa usanza.*

Facendo un bilancio quantitativo, con quello che avete in mano sono usciti sedici numeri, come dire 512 pagine, che trovate nella Secret Zone del sito Web in formato PDF. Sempre nella Secret Zone ci sono anche gli sfondi per scrivania con le immagini delle copertine (tanto per ricordare qualche aspetto che ci rende un po' speciali...). Per parlare ancora del sito, questo è stato completamente rinnovato e ampliato, e ospita ora un forum dove si possono scambiare opinioni e anche chiedere aiuto per i problemi tecnici.

Passando ai contenuti, credo che in questi ultimi mesi stiamo trovando un equilibrio tra i vari livelli di difficoltà. C'è sempre qualcuno che trova troppo difficile qualche articolo, e qualcun altro che invece dice che sono troppo semplici. Accontentare tutti con la stessa rivista però non è per niente facile.

Riguardo ai propositi per il futuro, qualche ideuzza ce l'abbiamo, e non vogliamo rovinarvi la sorpresa anticipandovela.

Ma siamo anche curiosi di conoscere la vostra opinione: come vorreste HJ? In cosa possiamo migliorare la rivista o il sito? Quali sono gli argomenti che vi interessano di più? Scriveteci le vostre impressioni: ne faremo tesoro per creare una rivista ancora più bella, ancora più unica.

Buon 2003!

grand@hackerjournal.it

Mezzogiorno di firewall

Il timer a Dasd City by passava tranquillo. Dopo l'ultimo processor ad un ladro di polling tutto sembrava quiet.

"Ehy, Job, brutto figlio di put, mi hanno detto che fai il default con Key, la mia ragazza!"

Nel saloon si giocava a card.
Appoggiato al benchmark, Job sorseggiava un punch fumando una cisc. Dal cinturone pieno di cartridge pending una Browsing 48K.
L'host stava pulendo con uno scratch una picture del Generale Cluster.
All'improvviso... shutdown!!!
Si open la port ed enter Blank, point il digit e disse:
"Ehy, Job, brutto figlio di put, mi hanno detto che fai il default con Key, la mia ragazza!"
"Output di qui e non mi rompere le labels else ti unpack il queue", response Job all'inquiry di Blank.
"Non fare il buffer, ti pare il modem di parlarmi?", disse Blank.
"Mettiamo le cause in sinclair e non fare il phase", lo interrupt Job, "Ho fatto il default con Key perche' tu la lasci sempre standalone e io la console. E lo faro' finche' mi fara' commodore!"
Ma aveva fatto l'acounting senza l'host...
Improvvisamente, Vtoc!... Vtoc!... Enter gli otto fratelli bit della banda Byte, amici di Blank, che avevano sentence tutto.
Job li view con la code dell'occours. Gli dissero:
"Ci display per te, ma ti faremo passare un brutto roscoe perche' sei un uomo senza password!!"
Job estrasse la sua 48K, la pointer contro di loro e fece Dump! Dump!
Input in quel momento Key, la ragazza di Blank, che crash colpita da Job.
Invano tentarono di rename, la stanby su un package abbastanza software e la fasciarono con della abend ma ormai la sua sort era signoff.
Chiamarono allora il padre Priority che la until con l'olio send; ma prima di memory risolta a Job disse, con un file di voice:
"Caro amico, questa e' la EOF; sii fortran: era sincom stare con te, dammi un ultimo batch!"
Job acconsenti' e la basic.
Appena terminal, Key expired branche al cobol di Job, diventando hardware senza possibilita' di restart... e la sua anima ascending al Cyl.
"Il delete non payroll..." mormoro' l'host scrolling la test.
Fuori tirava un vento flag. Il disk della luna si era retry fra le nuvole. Blank, Job e i fratelli Byte order all'host un drum che bevvero in un source.
Poi sysin camminarono con passo floppy e le mani in task lasciandosi alle spalle il saloon e la bella Key more...
Intanto init a piovere e si separarono alla search di un recovery per la not.
La storage di Key e' finita. Se return a Dasd City, record di visitare la tomba di Key per depending un mazzo di overflow.
Requiesce in Pause

"Output di qui e non mi rompere le labels else ti unpack il queue"

"Caro amico, questa e' la EOF; sii fortran: era sincom stare con te, dammi un ultimo batch!"

S4mWis3

Ndr: La storiella è carina, ma vecchiotta. La prima apparizione su Usenet è del 1998 (stando a quanto dice Google), ma qualcuno narra che girasse anche all'epoca della rete Fidonet. In ogni caso, è così divertente che abbiamo deciso di pubblicarla ugualmente.

UN GIORNALE PER TUTTI: SIETE NEWBIE O VERI HACKER?

NEWBIE

MID HACKING

HARD HACKING

Il mondo hack è fatto di alcune cose facili e tante cose difficili. Scrivere di hacking non è invece per nulla facile: ci sono curiosi, lettori alle prime armi (si fa per dire) e smanettoni per i quali il computer non ha segreti. Ogni articolo di Hacker Journal viene allora contrassegnato da un level: NEWBIE (per chi comincia), MIDHACKING (per chi c'è già dentro) e HARDHACKING (per chi mangia pane e worm).

mailto:
redazione@hackerjournal.it

ARRIVANO GLI ARRETRATI
Ho perso i primi numeri di HJ. So che si possono scaricare i Pdf dal sito, ma sono un feticista e voglio assolutamente completare la collezione su carta. Come posso fare per avere i numeri arretrati? Sono disposto a pagare anche il doppio o il triplo del prezzo di copertina… Aiutatemi!

Glamdring

E se noi addirittura te li facessimo pagare meno del prezzo di copertina? I nostri mezzi non ci consentono di avere un servizio arretrati con spedizione a domicilio, ma le richieste erano tante, per cui abbiamo deciso di porre in qualche modo rimedio a questa mancanza. A breve troverai in edicola "Hacker Journal Collection", la raccolta dei primi sei numeri della rivista. In seguito, verranno rese disponibili le raccolte dei numeri successivi.

MEMBRI CERCANSI
Sto cercando di formare una crew con lo scopo di creare un vero portale hacker. In particolare, ci serve qualcuno che sia esperto di grafica Web e qualche traduttore dall'inglese.
Ma anche esperti hacker, web master e intenditori di programmazione non guastano.
Per gli interessati scrivere a milo.cutty@libero.it

Milo Cutty

Voilà. Nel trovare nuovi membri, HJ è persino meglio di FermoPosta.

IL COSTO DI INTERNET
Tutti vogliono incentivare Internet, vogliono svilupparlo. Ogni giorno oramai si parla di Internet ma nessuno da la possibilità a noi comuni mortali di ridurre le spese de connessione, che secondo me sono eccessive. Non esistono tipi di abbonamenti a costo fisso, tranne quelli Adsl (per molti troppo costoso). E anche con Adsl, la copertura manca in buona parte del Paese. Non esistono abbonamenti a linea 56k come il vecchio Libero@sogno vi ricordate? Cosa dovremmo fare? Io per primo ho deciso di togliere il modem dal mio pc, e voi cosa fate: continuerete a pagare?
Spero che voi della redazione possiate aiutare o per lo meno consigliare tutti quelli che, come me, hanno deciso di fare questa scelta.

Vittore

È dal 95 che scrivo che la differenza principale tra l'uso di Internet negli USA e in Europa risiede nei costi di collegamento, che negli USA sono fissi mentre da noi variano in base al tempo di connessione. Detto questo, non bisogna però ignorare che anche negli USA il collegamento Internet ha un costo, che solitamente si aggira sui 20 dollari al mese. A questo va aggiunto il costo dell'abbonamento telefonico, più alto persino di quello della sanguisuga-Telecom: almeno un'altra ventina di dollari per un abbonamento con chiamate urbane gratuite. Siamo a 40 dollari al mese, 480 all'anno, o se preferisci quasi 950.000 delle vecchie lire.
È vero: i vecchi abbonamenti flat sono spariti (rimane ancora qualcosina, dalle caratteristiche ridotte rispetto al passato, come quelle che trovi su www.tariffe.it/free_internet_flat.htm). E le zone non attualmente coperte da Adsl difficilmente lo saranno a breve. Detto questo, per gran parte della popolazione sono accessibile abbonamenti Adsl a prezzi tutto sommato comparabili con quelli di un abbonamento americano su linea commutata.

CAMPASKONNETTI
Mi sono fatto una connessione internet, e dato ke la mia stanza è lontana dal telefono, ho fatto a modo mio e –attraverso battiscopa e pareti– il filo è invisibile… Non so se è mai capitato anche a voi, ma ora quando suona il mio campanello, vengo immediatamente disconnesso dalla Rete.
Convinto fosse una casualità, ho voluto provare, e sono certo che il mio campanello, è diventato CAMPASKONNETTI…
Infatti, ho verificato ke il suono da fastidio al fiskietto per la konnessione internet, e ke quando suona mi stacca la linea.
Voglio kiedervi se ne eravate gia a konoscenza, e se sekondo voi nn potrebbe diventare un'attacco ke skonnette la vittima, registrando questo suono e… Insomma, fatemi sapere

IL DJ ALATO: KINGOFDISKO

I suoni non c'entrano nulla. Sicuro di aver collegato i cavi per bene? Scommettiamo che il cavo del telefono passa vicino a quello del campanello? In questo caso, hai scoperto che esiste l'interferenza elettromagnetica.
Riguardo alla possibilità di usare il campanello per portare un attacco che scolleghi la linea, lascerei perdere: bisogna convincere la vittima a ricablare casa. Meglio usare una pistola EMP, che gli friggerà tutti gli apparecchi elettronici di casa. Quella mostrata all'indirizzo www.totse.com/en/bad_ideas/ka_fucking_boom/164724.html dovrebbe funzionare.

UNA LEGGE BACATA

Volevo segnalarvi un "bug" della legislazione italiana; è giusto secondo voi che uno che commette un "crimine" informatico (defacement, intrusione in un sistema, ecc.) si ritrova a scontare più anni di carcere di quanti ne sconti una persona che dopo aver ucciso si dichiara inferma mentale???
Poi … i provider che oscurano i siti hacker solo perché credono che i contenuti di questi siti rovinino la propria immagine.
Non è anche questa una forma di dittatura???
L'articolo 21 della nostra costituzione, che fine ha fatto???
Lascio la mia e-mail: imp3r4tor@libero.it così se qualcuno vuole rispondere alle mie domande può farlo.

Imperator

Anche nello scorso editoriale abbiamo parlato della sproporzione che a volte esiste tra la gravità dei reati informatici e le pene comminate. Ci schieriamo anche dalla tua parte anche per quanto riguarda la "censura preventiva" che certi provider adottano per i contenuti pubblicati negli spazi gratuiti. In questo secondo caso, però, vale una delle grandi regole di Internet: ognuno ha il diritto di adottare la politica e le regole che preferisce per l'utilizzo dei servizi che offre al pubblico. A maggior ragione se sono servizi gratuiti. Può piacere o no, ma "così è la Rete".

Nuova password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troverete informazioni e strumenti interessanti. Con alcuni browser, potrebbe capitare di dover inserire due volte gli stessi codici. Non fermatevi al primo tentativo.

user: bisc8
pass: 9llino

☺☺☺ TECH-HUMOR ☺☺☺

Questi messaggi sono presi in considerazione da Microsoft per Windows 3000:

1 Dai un forte colpo sulla tastiera per continuare.
2 Inserisci un qualsiasi numero primo di 11 cifre per continuare.
3 Premi un tasto qualsiasi per continuare o un altro tasto qualsiasi per uscire.
4 Premi un tasto qualsiasi… no, No, NO, NO QUELLO NO!
5 Premi Ctrl-Alt-Canc per testare il sistema.
6 Chiudi gli occhi e premi ESC tre volte.
7 Comando o nome di file errato. Subito in castigo!
8 Questo chiuderà la sessione di Windows. Vuoi giocare a un altro gioco?

9 Errore durante il salvataggio del file! Formattare il disco ora? (S/s)
10 Questo messaggio arriva dal Dio Gates: "Riavvio del mondo in corso… Per favore uscire."
11 Per spegnere il computer, entrare in Windows.
12 BREAKFAST.SYS bloccato… La porta ai cereali non risponde.
13 COFFEE.SYS mancante… Appoggiare una tazzina sul portatazze e premere un tasto per continuare.
14 CONGRESS.SYS corrotto… Riavviare Washington D.C? (S/N)
15 File non trovato. Posso inventarmelo? (S/N)
16 Mouse mancante. Hai lasciato in giro il gatto? (S/N)
17 Errore di runtime 6D all'indirizzo 417A:32CF: Utente incompetente.
18 Errore durante la lettura della FAT TURCHIN: provare con GEPPETT ? (S/N)
19 Porta stampante non trovata. La prossima volta fanne una copia di backup.
20 Errore di utente: cambiarlo.
21 Norton Antivirus 2000 - "E' stato trovato Windows 2000: rimuoverlo? (S/N)"
22 Benvenuti nel mondo Microsoft - il tuo contratto è già scaduto…
23 Il tuo disco è stato analizzato e tutti i programmi installati sono stati cancellati. La polizia è dietro l'angolo!

VIDEOPOKER, ADDIO

La commissione Bilancio del Senato ha approvato nuove regole per i videogiochi da bar: il gestore con macchine non in regola può ricevere sanzioni da 4000 fino a 40.000 euro. Ma la notizia più importante è che, dopo un tentativo di far passare una norma per isolare i videopoker in sale ad accesso riservato ai maggiorenni, la Commissione ha optato per il bando assoluto e totale. Se questo servirà ad arginare il fenomeno o a fa nascere sale clandestine, solo il tempo lo dirà…

LINUX SULLO SMARTPHONE

Ibm e Consumer Direct Link hanno lanciato Paron MPC, uno SmartPhone con sistema operativo basato su Linux. E' basato su un processore Intel StrongARM Sa-1110 da 206 Mhz con 64 MByte di Ram e 32 MByte di Rom, display a colori e GSM Dual Band 900/1800 Mhz con supporto GPRS, Wi-Fi e Bluetooth. Il sistema operativo è basato su Linux, con browser Opera, prediletto dai costruttori di SmartPhone. Misura 137 x 79 x 20 mm e pesa 250 grammi, e possiede un dispositivo di riconoscimento impronte digitali.

ARRIVA OROR-K

Un nuovo worm, poco diffuso per il momento, rappresenta un pericolo potenziale per la posta elettronica e le condivisioni in peer to peer, copiandosi nelle cartelle condivise e spedendosi agli indirizzi in rubrica. I subject, i messaggi e gli attachment sono variabili, ma tutti a sfondo umoristico/malizioso. La vulnerabilità sfruttata è sempre quella dell'autoesecuzione (ampiamente patchata). Quindi il virus si copia, mostrando un messaggio di errore fittizio, e copiando nel Registro le informazioni necessarie a diffondersi, cercando di bloccare gli antivirus.

COLPO GROSSO NEL REGNO UNITO

Un cracker è riuscito a penetrare nei sistemi di alcuni importanti tour operator britannici e a prelevare diverse decine di migliaia di sterline senza quasi lasciare traccia. L'audace operazione, considerata una delle violazioni più gravi mai avvenuta in Inghilterra, è stata effettuata mediante una backdoor inserita nei sistemi di pagamento. Grazie, si suppone, a una conoscenza approfondita del protocollo X.25 utilizzato dai sistemi Aix di importanti tour operator fra cui Sea France e Wightlink Holiday Placet, e all'utilizzo di programmi di gestione delle prenotazioni e dei pagamenti del tutto identici fra loro, l'hacker è riuscito a intercettare gli ordini di pagamento con carta di credito, trasferendo le somme su un conto aperto sotto falso nome oltreoceano e facendoli passare, a livello contabile, come rimborsi. L'operazione, quasi perfetta, è stata scoperta per via di una imperdonabile leggerezza: tutti i rimborsi "fittizi" erano in cifra tonda (3000 sterline e non, per esempio, 3243,67 sterline, caso molto più comune). Il fenomeno è stato notato da un operatore, che ha segnalato l'anomalia e permesso così di scoprire la backdoor. Nonostante ciò, l'hacker ha eliminato accuratamente le tracce del suo passaggio, e quindi diventa davvero difficile poterlo identificare.

TELEFONI BOMBA?

Va per la maggiore in questi giorni, su forum e newsgroup, una storia che ha il sapore della leggenda metropolitana, e che parla di un appello "ufficiale", firmato Total Fina, che paventa incendi e esplosioni se, per combinazione, un telefono cellulare si mettesse a squillare durante una operazione di rifornimento di benzina o Gpl presso un distributore.
In verità, da quando esistono i cellulari, sui manuali ci sono chiari avvisi di evitarne l'utilizzo e, anzi, di spegnerli in prossimità di pompe di benzina, ma tant'è, ci voleva il fattaccio per sensibilizzare la maggioranza. Fattaccio con tanto di descrizioni splatter: pantaloni in fiamme, visi ustionati, distributori esplosi, autovetture incendiate e via dicendo. Salvo poi, alla resa dei conti, scoprire che non ci sono tracce nella cronaca di questi episodi così truculenti. Solo un'altra leggenda metropolitana, con un fondo di verità: è sempre sconsigliato trafficare con apparecchi elettronici vicino a sostanze infiammabili.
Come al solito, tutti dicono la loro, ma nessuno può giurare su nulla. Nemmeno sulla veridicità dei fatti descritti. Se ne parla, magari anche ai distributori, e perché no, accendendosi una sigaretta appena scesi dall'auto…

TISCALI ABBATTE I DIALER

Abbiamo parlati qui più volte dei dialer, quei programmini un po' infidi nascosti fra link promettenti (tipo loghi e suonerie, per tacere di quelli più maliziosi..), e che, per farci accedere ai servizi promessi, staccano la nostra connessione, in modo più o meno subdolo, per collegarci a qualcosa di molto, molto più costoso. Tutto questo nell'impossibilità di fermare il fenomeno, ai limiti della legalità ma certo non onorevole, basato su un meccanismo che fa leva sull'ignoranza degli utenti. Gli addetti al lavoro alzano le spalle, puntando il dito sul fallimento delle vecchie forme di pubblicità tipo banner o popup e il bisogno di nuove fonti di reddito dalla Rete, traendoli da servizi che vogliono considerare, nella loro nebulosità, servizi premium. In Italia. All'estero i dialer sono severamente regolamentati.
Non facciamo commenti su questo vedere la Rete come una specie di gallina dalle uova d'oro. Vogliamo piuttosto dare rilievo alla notizia che Tiscali, fra i pionieri in Italia nei primi esperimenti di ecommerce, ha eliminato dai suoi server tutti i servizi riconducibili a dialer, rinunciando a introiti nell'ordine dei 10 milioni di euro. Tirino un sospiro di sollievo le famiglie angosciate dalle bollette astronomiche per le incaute navigazioni dei figli a caccia di suonerie: su Tiscali non si correrà questo rischio.

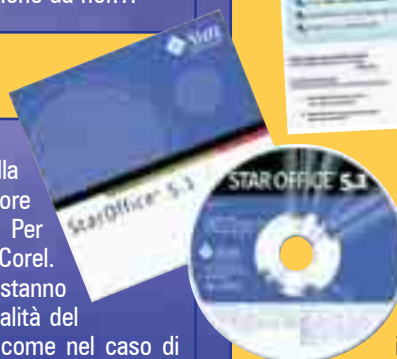
GALATEO MOBILE

E' uscito, edito da Lupetti, Mobile Etiquette, una interessante guida all'uso del cellulare, in forma di un vero e proprio galateo, scherzoso ma non troppo. La lettura può senz'altro strappare qualche sorriso, ma anche fare riflettere… e molto.
Prima di tutto, la risposta alla domanda fondamentale: possiamo permetterci di non utilizzare il cellulare? Sì, se siamo molto importanti e qualcuno lo può usare al nostro posto. Altrimenti, dobbiamo rassegnarci. Oppure utilizzare mezzi alternativi (è chiaramente precisato che la posta elettronica non lo è, mancando di immediatezza), come numeri di telefono fissi da chiamare a orari precisi (ma ne vale davvero la pena?).
Il telefono non deve essere sempre acceso, anzi. Ma la segreteria ci deve sempre essere. E con un messaggio personalizzato, in modo da rassicurare l'interlocutore sulla nostra identità. Indispensabili auricolare e vibracall, in modo da non disturbare chi ci circonda. E per lo stesso motivo il cellulare va sempre tenuto addosso nell'apposita custodia, mai appoggiato in giro, mai tenuto lontano: che non suoni mai a vuoto. E, infine, si badi sempre a utilizzarlo lontano dalle persone, uscendo da scompartimenti di treno e alzandosi da tavola, e utilizzando sempre il tono di voce giusto, per far capire all'interlocutore il proprio grado di disponibilità.

GIUDICI & SENTENZE

Non contenta di fare il poliziotto del mondo, l'America da un po' di tempo vuole fare anche il giudice globale. In questi giorni nelle aule dei tribunali americani si sono tenute udienze che vedono come imputati cittadini norvegesi e russi, accusati di aver violato leggi americane mentre erano nei loro paesi. Secondo la legge nota come Digital Millennium Copyright Act (DMCA), infatti, un crimine commesso sulla rete può essere punto secondo le leggi americane, indipendentemente dal paese in cui si trovava il reo. Un caso è quello della ElcomSoft, la software house russa che ha creato un programma per la gestione degli eBook di Adobe. Con questo programma, è possibile rimuovere la protezione inserita negli eBook, rendendo il loro contenuto accessibile senza bisogno di password. L'accusa ha cercato di provare che ElcomSoft ha deliberatamente e volontariamente creato un software illegale, ma ha perso la causa. La difesa infatti ha puntato l'attenzione sul fatto che è assurdo che un'azienda produca, promuova con comunicati stampa e cerchi di vendere sul mercato un prodotto, se sa che questo non rispetta le leggi.
Non altrettanto bene sta andando al norvegese Jon Johansen, che all'età di 15 anni ha infranto la protezione dei DVD, con il suo software DeCSS. Johansen ha sempre sostenuto di averlo fatto per poter finalmente vedere i DVD sul suo sistema Linux (fino ad allora non c'erano software per farlo), e per di più per la legge norvegese non è un reato decifrare un DVD regolarmente acquistato. L'accusa ha chiesto una pena di 90 giorni di carcere, ma la sentenza arriverà solo verso la metà del mese. Ora, in alcuni stati USA è viatato il sesso orale: speriamo che a nessun giudice venga in mente di perseguire questo reato anche da noi…

SONY PASSA A STAROFFICE

Dalla fine di quest'anno, sui Pc prodotti da Sony verrà installata, al posto della tradizionale suite Works, StarOffice 6.0. Ed è solo uno dei tanti produttori del settore (seppure, fino ad oggi, il più importante) ad aver scelto soluzioni alternative. Per esempio, Hp e Dell hanno sostituito Office e Works con Wordperfect Office 10 di Corel. L'erosione dell'egemonia di Microsoft si sta facendo sentire: le suite "parallele" stanno creando una vera e propria concorrenza al colosso di Redmond, vuoi per la qualità del tutto paragonabile, vuoi soprattutto per il costo, irrisorio o del tutto gratuito, come nel caso di OpenOffice.
StarOffice 6.0, infatti, include un elaboratore di testi, Writer, un foglio elettronico, Calc, un generatore di presentazioni, Impress, e un database, e gode di una vasta gamma di compatibilità con varie piattaforme. E' simile per interfaccia a Office, è compatibile con i suoi formati e supporta Xml. Ed è in corso lo sviluppo di uno standard per i formati dei file a cura di Corel e Sun, in modo da migliorare l'interscambio di file fra i diversi applicativi e di applicazioni fra diverse piattaforme.

ORDINARIA FOLLIA TELEMATICA

Un trentenne scozzese è stato processato per aver aggredito e percosso un amico del proprio fratello, accusandolo di avergli inserito un virus nel computer attraverso un dischetto. Il ragazzo era al lavoro per collegare i due computer di casa in rete, quando il suo aggressore ha trovato un dischetto contenente, a suo dire, un programma backdoor. Al che ha impugnato un'ascia e si è avventato sul malcapitato tecnico, colpendolo, per fortuna di striscio, alla testa.

FALLA IN REAL PLAYER

Si tratta di un buffer overrun, una delle più caratteristiche falle di Explorer, legata ai nomi lunghi, che possono portare a "semplici" crash o, nei casi peggiori, all'esecuzione di codice maligno sul pc ospite. Non sono stati comunque ancora riportati casi di attacchi riusciti. Ad ogni modo, sul sito Real si posso trovare le istruzioni per patvhare le varie versioni (http://service.real.com/help/faq/security/bufferoverrun.html)

IL NUOVO ICQ

Con l'uscita della versione 2003a di Icq si è fatta più netta la differenza fra Icq tradizionale (ora chiamato Pro) e Lite, senza moduli aggiuntivi oltre al semplice instant messaging. Queste due versioni vanno a coprire virtualmente tutte le esigenze di instant messaging, sulla maggior parte delle piattaforme (Palm, Pocket PC, Mac, Ce, Nokia Communicator, compatibilità con analoghi programmi Windows).

UNO SGUARDO AL FENOMENO DEL SOCIAL ENGINEERING

Lei non sa chi sono io...

Una delle tecniche principe di spie e agenti segreti è sempre stata quella di fingersi qualcun altro per avere accesso a informazioni riservate. Un sistema molto in voga anche tra cracker e ladri di informazioni.

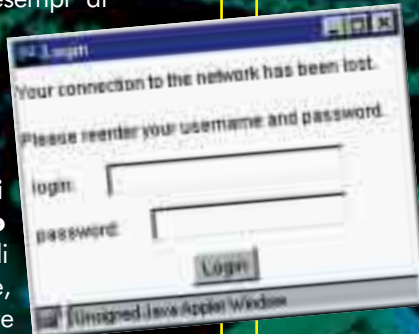
"Social engineering" è termine intraducibile per indicare tutta quella gamma di **trucchi psicologici utilizzabili per convincere qualcuno a rivelarci i suoi dati di accesso** a un sistema o simili. Ed è una forma di cracking tanto più sgradevole in quanto **colpisce un lato molto nobile e sempre più raro dell'animo umano: la tendenza a fidarsi del proprio prossimo**.

>> Amici o nemici?

```
"Ciao, Mario. Sono Stefano
del Ced. Ho finalmente la
nuova versione del programma
di posta. Basta blocchi :)
Mi ricordi al volo il tuo
username e password, così
non devo stare a scartabel-
lare negli elenchi che non
mi passa più? Grazie ;)"
```

Mail rilassata, simpatica, carina, apparentemente innocua. Apparentemente. *Quasi come la telefonata che recita: "Antonella? Sono Daniele, lo stagista del Ced, sono fuori da un cliente e c'è il server giù, ti spiace loggarti con l'account da amministratore e premere qualche tasto? Grazie, cara".*
Per non parlare di quello che è considerato uno dei "capolavori" del social engineering:
"Buongiorno, chiamo dalla (nome di provider di telefonia), volevo avvertirla che le sue chiamate verso la Tunisia stanno superando la soglia di credito... come dice? Lei non ha mai chiamato la Tunisia? Ma a display mi risulta una chiamata in atto... accidenti, è impossibile, ci deve essere un errore... ascolti, mi dia i dati della sua carta telefonica che le scarico subito la cifra... sono quasi duemila euro, sa com'è, non dovrei farlo ma se facciamo alla svelta prima che arrivi il mio collega..."
Questi sono solo esempi di tanti altri messaggi e azioni possibili, tutti con il solo scopo di **far inviare senza troppa esitazione i nostri dati al truffaldino di turno**: richieste di file di configurazione, backdoor spacciate per patch eccetera.
E tutti, indistintamente, basati sul principio **"vengono fatti sistemi a prova di utente sbadato, ma gli sbadati sono ingegnosi"**. Come dice lo stesso Mitnick, inutile dotare un'azienda di un firewall inviolabile, quando le aggressioni non sono dirette al sistema ma ai suoi utenti umani, molto più vulnerabili di qualunque macchina.

>> Anche dal vivo

Molto diffusi sono anche i casi di social engineering "live": simpatiche signore che girano per le aziende, senza che nessuno gli rivolga neppure la parola, raccattando foglietti gialli adesivi dai monitor. Per non parlare dello "shoulder surfing", come è chiamata la diffusa tecnica di occhieggiare, da sopra la spalla di un impiegato, l'immissione di username e password. O, meglio ancora, il "dumpster diving", che è, banalmente, **frugare in cestini e bidoni alla ricerca di appunti** volanti, ricevute, stampate, hard disk guasti, elenchi di impiegati, piani ferie....
Gli stessi virus diffusi via email fanno leva su ancestrali esigenze dell'essere umano. Si pensi al virus LoveLetter, che annunciando "Qualcuno ti ha inviato in allegato una lettera speciale! Leggila!" ha fatto una strage di destinatari speranzosi o anche solo curiosi.

>> Relazioni pericolose

La letteratura in materia di social engineering rivela che sotto celebri violazioni o clamorosi blackout informatici di grandi aziende o importanti provider a livello internazionale c'erano situazioni apparentemente innocue e molto umane, ma sfruttate con malizia dall'intrusore. Un noto esempio è quella della classica amicizia coltivata via chat da parte di un'ignara impiegata di un noto provider statunitense, culminata con uno scambio di foto, come capita sempre in questi casi: l'impiegata spedì la propria foto, il suo amico di chat un virus trojan.
E forse per il fatto che è difficile ammettere di aver aperto e letto con avidità una missiva dal titolo così idiota, o di aver chiamato il numero che compariva in fondo a un SMS che recitava più o meno "qualcuno ti ama in segreto e ci ha incaricato di comunicartelo, chiama qui", o di aver eseguito il dialer che ci fa navigare fra suonerie e donnine nude chiamando direttamente le Isole Vergini, il fenomeno sembra meno dif-

fuso di quanto non sia (molte sono anche le vittime ignare, che non penseranno mai a quel ragazzo così simpatico e curioso come a un cracker, neppure ad attacco avvenuto), e questo stimola da una parte la sua messa in atto, e dall'altra limita le contromisure.

>>Come difendersi

La prima cosa da fare per evitare di cadere in queste trappole è informarsi, informarsi, informarsi. Non si verrà additati, sghignazzando, se si chiede un chiarimento su una carica, un responsabile o una procedura. Né la nostra dignità professionale verrà sminuita: il truffaldino di turno potrebbe irretirci con istanze di cui non siamo tenuti a sapere, ma su cui è sempre bene chiedere prima di fare cose di cui potremmo pentirci; o addirittura impietosirci, o farci arrabbiare, o minacciarci.
E prima ancora, ragionare, ragionare, ragionare. Nessuno ci regalerà un cellulare di ultimo modello se riempiamo un formulario di dati sensibili riguardanti la nostra azienda o la sua dotazione di firewall e antivirus, così come nessuno ha davvero bisogno della nostra password se ha accesso al sistema come amministratore. In generale, chi si occupa di sistemi informativi dovrebbe periodicamente ricordare ai propri utenti che la password va custodita gelosamente e cambiata spesso (e MAI utilizzata per più di un account: **un noto metodo di social engineering è quello di invitare impiegati a registrarsi a servizi fittizi chiedendo un nome utente e una password, che spesso viene scelta, per pigrizia, uguale a quella dei servizi aziendali**), e non rivelata a nessuno in nessuna circostanza, a qualsiasi titolo si presenti, tanto più in virtù delle recenti normative sulla privacy. Questo vale ancora di più se la nostra password consente un accesso privilegiato a dati aziendali o riguardanti altre persone: si potrebbe incorrere, oltre che in guai professionali, anche, in casi limite, a una denuncia per "incauta custodia". Sì, quella stessa che venne alla ribalta qualche anno fa, quando una sbadata organizzatrice di serate con accompagnatrice per Vip smarrì la sua agenda telefonica, piena di nomi e riferimenti imbarazzanti.

>> Istruire i colleghi

Se siamo noi stessi a gestire le policy di un'azienda, oltre a mettere in atto le opportune, aggiornate misure di sicurezza, creiamo accessi il più differenziati possibile, per evitare l'eccessiva presenza di accessi "totali", con conseguente maggior pericolo di violazione (in parole povere, aumenta la percentuale di eventuali "sbadati", che possono cadere in trappole di social engineering). E, inutile dire, siano bacchettati fortissimo sulle mani tutti quelli che lasciano in giro foglietti con username e password. O che aprono con il proprio badge porte ad accesso riservato a sconosciuti che dichiarano di "averlo dimenticato in macchina" (succede, anche troppo spesso, sempre grazie al timore di "non ricordare la faccia di un collega e farci la figuraccia").
È doveroso dirlo: fare social engineering è anche troppo facile. Si può creare una pagina fittizia, navigando sulla quale l'utente riceve il popup "utente scollegato, reinserire username e password per collegarsi alla rete" o qualcosa del genere. O, molto più semplicemente, si possono ottenere dati importanti con una semplice telefonata.
Facciamo un esempio: una conversazione tipo fra una segretaria e un interlocutore standard.
"Buongiorno, sono Paolo Lamerini, c'è il dottor Caruso?"
"No, è in ferie fino al 28".
"Ah… Con chi posso parlare allora?"
"Può rivolgersi al dottor Mariani".
A questo punto il nostro Paolo Lamerini ha avuto delle informazioni incredibilmente preziose da parte della ignara segretaria. Non vi pare? Vediamo subito come potrebbe svolgersi la successiva telefonata di Lamerini.
"Mariani? Sono Lamerini, dello Studio Blue Box. Caruso mi ha detto che lui stava via e di parlare con lei, se c'erano urgenze, ecco, purtroppo ci è saltata una macchina e ci siamo persi il planning del progetto Arcadia, può faxarmelo urgentemente allo 00-123456? Grazie, gentilissimo!"
Niente male. Poche informazioni da ognuno, per non insospettire, poche ma fondamentali. Meglio fare attenzione. Molta attenzione. Sempre.

Paola Tigrino

Ognuno ha il suo punto debole

I truffatori si sono specializzati nel trovare il punto debole di ogni persona: qualcuno sarà più sensibile a una richiesta proveniente da una fanciulla, tipo:
"Ehm… scusa… ciao… mi chiamo Sonia… ho una mail farfallina@lammah.xx, aspetto TROPPO una mail importante e mi sono persa la password… ti prego… ti prego… io DEVO leggere quella mail, daiiiiiiiii….."
Con altri invece si potrà far leva sul senso del dovere e sul timore verso un capoufficio, con una telefonata tipo questa:
"Pronto? Bianchi? Io mi sono stancato, il capo è furioso, o si sblocca la sua mail o viene giù a fare un casino, dammi 'sta cavolo di password e facciamola finita, no! Adesso! Non mi frega se a te funziona tutto! Dammi quella password per carità, che gli stampo le sue mail e così si calma…"

Kevin Mitnick

Per la prima volta in italiano, e in versione integrale, il primo capitolo del libro del "Condor", censurato dal suo editore nella versione finale.

Lo scorso ottobre, negli Stati Uniti è uscito il libro "The Art of Deception: Controlling the Human Element of Security " (l'arte dell'inganno: controllare l'elemento umano della sicurezza), uno di quei libri che è già un successo ancor prima di toccare gli scaffali. Il motivo è presto detto: l'autore è Kevin Mitnick, l'hacker più ricercato (e più severamente punito) dal sistema giudiziario americano. E, in effetti, immediatamente dopo la pubblicazione, il libro ha fatto subito parlare di sé. Curiosamente però, la gente non parlava tanto di quello che c'era nel libro: parlava piuttosto di quello che nel libro non c'era. O meglio, di quello che non c'era più.

Nelle copie preliminari distribuite ai giornalisti prima della pubblicazione definitiva, infatti, si poteva trovare un capitolo in più rispetto a quelli che compongono la versione che si trova in libreria. Un capitolo che era stato frettolosamente rimosso prima della stampa finale.

Si sa però come vanno le cose nell'Era di Internet: è impossibile limitare la libera circolazione di qualsiasi materiale. E, anzi, quando si cerca di censurare, di vietare, di bandire qualche cosa, si ottiene come unico risultato quello di attirare su di esso l'attenzione delle persone. Ecco quindi che "il capitolo perduto" ha cominciato a circolare in mailing list e decine di mirror, e forse al momento attuale lo hanno letto molte più persone di quante abbiano comprato l'edizione ufficiale del libro.

Non sono chiari i motivi che hanno spinto l'editore a cassare il primo capitolo dal libro di Mitnick, probabilmente il più polemico verso il sistema giudiziario e dei media americani. Forse non si voleva dare l'impressione di voler condonare quello che è stato per anni (a torto o a ragione) uno dei criminali informatici più temuti e ricercati. Forse si volevano evitare le grane con il New York Times e il suo giornalista John Markoff, che Kevin accusa di averlo diffamato per vendetta, dopo il suo rifiuto a collaborare alla redazione di un libro.

Noi non vogliamo avallare le posizioni di Mitnick contro Markoff, o avvalorare le sue tesi. Pensiamo però che i lettori abbiano il diritto di sentire tutte le campane. Soprattutto è importante sentire quelle che i poteri forti hanno sempre cercato di zittire. Per questo, abbiamo tradotto il famigerato "Capitolo 1", e lo pubblichiamo integralmente in queste pagine straordinarie. Passiamo quindi la parola a Kevin. Buona lettura.

grand@hackerjournal.it

>> Capitolo 1: La storia di Kevin

Ho scritto questo capitolo con riluttanza perché sarebbe certamente apparso come qualcosa di auto celebrativo. Ma centinaia di persone mi hanno contattato per sapere: "chi è Kevin Mitnick".

Tutti quelli a cui non frega niente di tutto ciò, possono saltare direttamente al capitolo 2. Per tutti gli altri, per quello che vale, questa è la mia storia.

>> Parola di Kevin

Alcuni hacker distruggono file o interi dischi rigidi della gente. Questi vengono chiamati "cracker", o vandali.
Alcuni hacker alle prime armi non perdono tempo ad imparare la tecnologia: si limitano a scaricare programmi per ottenere accesso a computer. A questi ci si riferisce come "script kiddies".
Hacker più esperti e capaci di programmare, realizzano programmi e li rendono pubblici attraverso web e forum di discussione. Poi ci sono individui che non hanno interesse nella tecnologia, usano il computer semplicemente come un mezzo per aiutarli a rubare soldi, beni o servizi.
Malgrado il mito "Kevin Mitnick" creato dai media, io non sono un hacker cattivo. Quello che ho fatto non era neanche illegale quando cominciai. Diventò illegale solo dopo che fu approvata una nuova legge. Io continuai noncurante di ciò, e mi beccarono.
Il modo con in cui fui trattato dal governo federale non commisurato al tipo di crimine, ma aveva l'obiettivo di fare di me un esempio. Non mi meritavo di essere trattato come un terrorista o un criminale violento; di avere la mia casa perquisita con un mandato di perquisizione "in bianco"; di essere sbattuto in cella d'isolamento; di aver stralciati i diritti fondamentali normalmente garantiti a chiunque sia accusato di un crimine; di vedermi negata non solo la possibilità di ottenere libertà provvisoria, ma addirittura il diritto a un'udienza che mi permettesse di chiederla. E di essere costretto a passare anni lottando affinché il governo mettesse a disposizione dei miei avvocati d'ufficio le prove portate contro di me, così che si potessero preparare e difendermi.
Che ne è stato del mio diritto ad un processo veloce? Per anni, ogni sei mesi, mi sono state presentate due opzioni: "o firmi per rinunciare al tuo diritto costituzionale a un processo veloce, o vai sotto processo con un avvocato che non è preparato". Io decisi di firmare.
Ma forse sto andando un po' troppo in la con la mia storia.

>> L'inizio

La mia strada probabilmente è stata segnata fin dai primi anni di vita. Ero un ragazzino spensierato, ma annoiato. Mio padre ci lasciò quando avevo 3 anni e mia madre cominciò a lavorare come cameriera per mantenerci. Incontrarmi allora, figlio unico cresciuto da una madre che lavorava lunghe giornate senza orari fissi, voleva dire incontrare un ragazzino che stava da solo quasi tanto tempo quanto ne passava da sveglio. Ero la babysitter di me stesso.
Il fatto di crescere nella comunità di San Fernando Valley mi permise di esplorare l'intera Los Angeles. Prima dei dodici anni avevo imparato a viaggiare gratis nell'intera area metropolitana di L.A.
Un giorno, viaggiando sull'autobus, mi resi conto che l'intero funzionamento dei trasporti era basato sul particolare disegno del punzone buca carta che il guidatore utilizzava per segnare giorno ora e percorso nei biglietti di transito. Un guidatore amichevole, rispondendo a domande opportunamente studiate, mi disse dove avrei potuto comprare quel tipo speciale di buca carta.
I biglietti di transito dovrebbero permetterti di cambiare autobus e continuare verso la tua destinazione; io imparai come utilizzarli per viaggiare gratis dovunque volessi andare. Ottenere biglietti in bianco era una passeggiata: i bidoni della spazzatura vicino al capolinea erano sempre pieni di blocchi di biglietti di transito parzialmente usati, che i guidatori gettavano alla fine della loro giornata di lavoro.
Con un blocchetto in bianco e il buca carta, potevo creare biglietti di transito a piacimento e viaggiare dovunque gli autobus di Los Angeles portassero.
Presto memorizzai quasi tutte le rotte e orari degli autobus. Questo è uno dei primi esempi della mia straordinaria memoria per un certo tipo di informazioni; ancora oggi posso ricordare numeri di telefono, password e cose simili andando indietro fino alla mia infanzia.
Un altro interesse personale che apparve presto negli anni fu la mia passione per i giochi di prestigio. Appena imparato un nuovo trucco lo provavo e riprovavo fino a esserne padrone. In un certo senso, fu attraverso la magia che scoprii il piacere nell'imbrogliare la gente.

>> Dagli scherzi telefonici all'hacker

Il mio primo incontro con quella che sarebbe poi stata chiamata "ingegneria sociale" avvenne mentre frequentavo le superiori, quando conobbi uno studente che era coinvolto in un passatempo chiamato phone phreaking. Il phone phreaking è simile all'hacking, ma riguarda il sistema telefonico. Permette di esplorare le connessioni telefoniche sfruttando il sistema e gli impiegati della compagnia telefonica.
Mi mostrò interessanti cose che potevano essere fatte con un telefono, come accedere alle informazioni che la compagnia dei telefoni mantiene dei propri clienti, e l'uso di un numero di prova segreto per fare chiamate interurbane gratis. Solo più tardi scoprii che in realtà era gratis solo per noi, visto che in effetti non era un numero segreto di prova: le chiamate erano fatturate nella bolletta MCI di una sventurata società.
Questo fu il mio battesimo nel campo dell'ingegneria sociale. Il mio asilo, per modo di dire. Questo ragazzo e un altro phone phreak, che incontrai poco dopo, mi permisero di ascoltarli mentre realizzavano chiamate-pretesto alla compagnia dei telefoni. Io ascoltai le cose che dicevano per rendersi credibili, imparai dei diversi uffici delle compagnie telefoniche, vocaboli e procedure.
Ma l'apprendistato non durò a lungo; non ce n'era bisogno. Presto facevo tutto da solo, imparando con la pratica, facendolo anche meglio di coloro che mi avevano insegnato.
Il corso, che la mia vita avrebbe preso nei successivi quindici anni, era segnato.
Uno dei miei scherzi preferiti era quello di ottenere l'accesso non autorizzato a una centralina telefonica, e cambiare il tipo d'accesso a un altro phone phreak. Quando questi avesse tentato di fare

una telefonata, un messaggio registrato gli avrebbe chiesto di depositare 10 centesimi, quel numero risultava essere un telefono pubblico.
Mi tuffai in tutto quello che aveva a che vedere con la telefonia, non solo per quanto riguardava l'elettronica, le centraline e i computer, ma anche l'organizzazione dell'azienda, le modalità e i vocaboli. Dopo un po' probabilmente ne sapevo di più di ogni singolo impiegato della compagnia telefonica. Inoltre avevo sviluppato le mia capacità di "ingegnere sociale" in maniera tale che, a diciassette anni, ero in grado di convincere quasi qualsiasi impiegato della Telco a fare qualsiasi cosa, sia al telefono che faccia a faccia.
La mia carriera di hacker cominciò quando andavo alle superiori. Allora usavamo il termine hacker per intendere una persona che passava molto tempo maneggiando hardware e software per realizzare programmi più efficienti o per evitare passi non necessari e terminare il lavoro più rapidamente. Il termine ha ora connotazioni molto negative, e ha il significato di "criminale informatico". In queste pagine uso il termine nella maniera in cui l'ho sempre utilizzato, nel significato iniziale, benigno, del termine.
Alla fine del 1979, un gruppo di hacker di mia conoscenza che studiava al Los Angeles Unified School District, mi sfidò a entrare nell'Arca, il sistema di computer della Digital Equipment Corporation, usato per sviluppare RSTS/E, il loro sistema operativo. Io volevo essere accettato da questo gruppo in quanto volevo poter far domande e imparare cose nuove sui sistemi operativi.
Questi nuovi "amici" erano riusciti a impadronirsi del numero per chiamare il sistema di computer di Digital. Loro sapevano che il numero di telefono da solo era inutile, e che senza uno username e una password non sarei mai riuscito ad entrare.
Ebbene, questi tizi stavano per scoprire che, quando sottovaluti gli altri, tutto si può ritorcere contro di te e morderti nel culo. In realtà per me, anche a quella giovane età, l'idea di entrare nel sistema DEC era un grande stimolo. Fingendomi Anton Chernoff, uno dei principali programmatori del sistema, feci una semplice telefonata al system manager. Dissi che non mi era possibile accedere al sistema utilizzando uno dei miei account. Fui così convincente che l'interlocutore mi diede l'accesso e mi lasciò scegliere una password.
Come ulteriore livello di protezione, chiunque si connettesse al sistema, doveva avere anche una password di connessione. L'amministratore di sistemi me la diede. La password era "buffone", che, credo, possa descrivere come lui si sentì più tardi, quando scoprì cosa era accaduto.
In meno di cinque minuti avevo ottenuto accesso al sistema di sviluppo RSTE/E della Digital. E non ero connesso come un utente qualsiasi, ma come uno con tutti i privilegi che corrispondono a un programmatore del sistema.
In un primo tempo, i miei sedicenti "amici" si rifiutarono di credere che fossi riuscito a entrare nell'Arca. Uno di loro chiamò il numero e mi piazzò la tastiera di fronte con uno sguardo di sfida. Restò con la bocca aperta quando io entrai con accesso privilegiato. Più tardi venni a sapere che lo stesso giorno, dopo essersene andati, cominciarono a scaricare il codice sorgente dei componenti del sistema operativo DEC. Venne il mio turno per essere battuto. Dopo aver scaricato tutto il software che volevano, chiamarono il dipartimento di sicurezza della DEC affermando che qualcuno si era introdotto nel network della società. Diedero il mio nome. I miei cosiddetti "amici", prima utilizzarono i miei accessi per copiare codice sorgente molto importante, poi mi denunciarono.
C'era una lezione da imparare qui, ma non una che avrei imparato facilmente. Negli anni a venire mi sarei spesso cacciato nei guai per il fatto di essermi fidato di persone che pensavo fossero miei amici.
Dopo la scuola superiore studiai informatica al Computer Learning Center di Los Angeles. In pochi mesi il computer manager della scuola si rese conto che avevo scoperto una vulnerabilità del sistema e ottenuto tutti i privilegi nel loro minicomputer dell'IBM. I migliori esperti informatici impiegati dalla facoltà non potevano capire come avessi potuto farlo. In una maniera che forse è uno dei primi esempi della odierna politica che punta ad assumere gli hacker, mi fu fatta un'offerta che non potevo rifiutare: realizzare un progetto per migliorare la sicurezza del sistema della scuola o essere sospeso per essermi introdotto senza autorizzazione nel sistema. Ovviamente scelsi il progetto, e alla fine mi diplomai con lode.

>> Diventare un ingegnere sociale

Alcune persone si svegliano ogni mattina odiando la loro routine giornaliera, lavorando nella proverbiale miniera di sale. Io sono stato fortunato, il mio lavoro mi è sempre piaciuto. In particolare non potete neanche immaginarvi il senso di sfida, riconoscimento e piacere che ottenni nel periodo in cui lavorai come detective privato. Stavo raffinando le mie capacità nell'arte chiamata ingegneria sociale, o "come far sì che qualcuno faccia cose che normalmente non farebbe per uno sconosciuto", e venivo anche pagato.
Per me non è stato difficile apprendere l'ingegneria sociale. Da parte di mio padre, la mia famiglia era stata composta da venditori fin da generazioni: forse l'arte di persuadere e influenzare faceva parte dei miei tratti ereditari.
Quando combini un'inclinazione naturale nell'ingannare la gente con l'arte di persuadere e influenzare, trovi il profilo dell'ingegnere sociale.
Ci sono due specialità nella classificazione del lavoro di truffatore. Uno che truffa e frega i soldi alla gente appartiene alla sotto categoria degli imbroglioni. Uno che utilizza astuzia, influenza e persuasione contro compagnie, di solito avendo come obiettivo le loro informazioni, appartiene a un'altra sotto categoria: quella degli ingegneri sociali.
Fin dal tempo dei miei trucchi con i biglietti degli autobus, quando ero troppo giovane per sapere che c'era qualcosa di sbagliato in quello che stavo facendo, imparai a riconoscere in me un talento per scoprire i segreti che non avrei dovuto conoscere. Costruii la mia vita

su quel talento con astuzia, conoscenza dei vocaboli, e sviluppando una ben meritata capacità di manipolazione. Una sistema col quale ero solito lavorare per sviluppare le mie capacità in questo hobby (se di hobby si può parlare) era quello di scegliere un qualche tipo di informazione per la quale non avevo un reale interesse, e vedere se riuscivo a convincere la persona dall'atro capo della cornetta a fornirmela, tanto per migliorare il mio talento.
Allo stesso modo praticavo i miei trucchi magici: per puro diletto. Attraverso queste pratiche presto scoprii che potevo entrare in possesso di quasi ogni tipo di informazione volessi.
In una testimonianza che resi anni dopo al Congresso, davanti ai senatori Lieberman e Thompson, dissi: "Ho ottenuto accesso non autorizzato nei sistemi di computer delle società più importanti del pianeta, con successo sono penetrato alcuni tra i sistemi più sicuri mai sviluppati. Ho utilizzato sia metodi tecnologici che non, per entrare in possesso di codici sorgente di vari sistemi operativi e di apparecchi per la telecomunicazione, per studiarne le vulnerabilità e il loro funzionamento interno". Tutto questo era semplicemente per soddisfare la mia curiosità, vedere che cosa fossi in grado di fare, e scoprire informazioni segrete sui sistemi operativi, telefoni cellulari, o qualsiasi altra cosa che stuzzicasse la mia curiosità.
Il vortice di eventi che trasformò la mia vita cominciò quando, il 4 luglio 1994, divenni il protagonista dell'articolo principale della prima pagina del New York Times. Da un giorno all'altro, quella storia cambiò la mia immagine da quella di hacker da strapazzo poco conosciuto in quella di "nemico pubblico numero uno del cyberspazio".

>> John Markoff, il truffatore dei media

"Kevin Mitnick è un programmatore di computer uscito di senno che combina il talento tecnico con gli antichi trucchi del truffatore. (dal New York Times, 4/7/94)". Combinando l'antico desiderio di ottenere un successo immeritato, con il potere di pubblicare informazioni false e diffamatorie sul suo soggetto nella prima pagina del New York Times, John Markoff è un reporter hi tech uscito di senno.
Markoff guadagnò oltre un milione di dollari per aver creato dal nulla quello che io chiamo "il mito di Kevin Mitnick". Diventò ricco proprio con la stessa tecnica che io usai per introdurmi nei sistemi di computer e network nel mondo: l'inganno. In questo caso, però, l'ingannato non era un singolo amministratore di sistemi o utilizzatore di computer, ma ogni persona che credeva nelle notizie pubblicate sulle pagine del New York Times.
Il super ricercato del cyberspazio, l'articolo scritto da Markoff e pubblicato sul Times, era ovviamente scritto per ottenere un contratto per un libro sulla storia della mia vita. Io non ho mai incontrato Markoff, ma lui è letteralmente diventato milionario grazie ai "rapporti" su di me, diffamatori e tendenziosi, che pubblicò prima nel Times e poi, nel 1991, nel suo libro "Cyberpunk".
Nel suo articolo egli incluse una dozzina di supposte verità su di me, che incluse come fatti senza citare alcuna fonte, e che, anche un minimo processo di ricerca dei fatti (che credevo fosse una pratica che tutte le pubblicazioni di un certo livello richiedesse ai loro giornalisti) avrebbe rivelato come false o non provate.
In quel solo articolo, falso e diffamatorio, Markoff mi rappresentò come "il cyberpunk più desiderato dalle forze dell'ordine", e come "uno dei maggiori criminali di computer ricercati dalla polizia in tutta la nazione", senza giustificazioni, ragioni, o prove, utilizzando meno discrezione di chi scrive il volantino pubblicitario del supermercato.
Nel suo articolo calunniatore, Markoff sostenne falsamente che io avessi spiato l'FBI (non l'ho fatto); che mi fossi introdotto nei computer di NORAD (che non sono neanche connessi a un network esterno); e che io fossi un vandalo del computer malgrado il fatto che io non abbia mai intenzionalmente danneggiato un computer al quale mi sia connesso. Queste e altre affermazioni erano completamente false e scritte con l'intento di creare un senso di paura delle mie capacità.
Rompendo, una volta di più, l'etica giornalistica, Markoff non rese nota in quell'articolo né in tutti gli articoli successivi, il fatto che tra noi due c'era già stata una relazione; un'animosità personale basata sul mio rifiuto di partecipare al libro "Cyberpunk". Inoltre gli ero costato un bel po' di potenziali guadagni, rifiutando di rinnovare l'esclusiva per un film basato sul libro. L'articolo di Markoff era chiaramente mirato a provocare le forze dell'ordine americane.
"Le Forze dell'ordine non sembra siano in grado di stare al passo con lui" scrisse. L'articolo era deliberatamente creato per inquadrarmi come il nemico pubblico numero uno del cyberspazio, in maniera tale che il dipartimento di giustizia avrebbe aumentato la priorità data al mio caso.
Alcuni mesi più tardi, Markoff e Tsutomu Shimomura, il suo socio, parteciparono al mio arresto come agenti di fatto, in violazione sia delle leggi federali sia dell'etica giornalistica. Entrambi erano nelle vicinanze quando tre permessi di perquisizione in bianco furono usati per frugare illegalmente casa mia, e in occasione del mio arresto. Durante la loro investigazione, i due violarono la legge intercettando una mia telefonata personale.

Mentre mi dipingeva come "il cattivo", Markoff, in un articolo successivo, introdusse Shimomura come l'eroe numero uno del cyberspazio. Ancora una volta, violava l'etica giornalistica non rendendo pubblica una relazione pre-esistente: l'eroe era da anni un intimo amico di Markoff.

>> Il primo contatto

Il mio primo incontro con Markoff avvenne alla fine degli anni ottanta, quando lui e sua moglie si misero in contatto con me mentre scrivevano il libro Cyberpunk, che avrebbe dovuto essere la storia di tre hacker: un ragazzo tedesco chiamato Pengo, Robert Morris e io. Quale sarebbe stato il mio compenso per partecipare? Niente. Non vidi motivo di dare a loro la mia storia se loro ne avrebbero guadagnato e io no, quindi rifiutai di aiutarli. Markoff mi diede un ultimatum, fai un'intervista con noi o qualsiasi cosa che ci venga detta da qualsiasi fonte sarà considerata vera. Era ovviamente frustrato e irritato dal fatto che io non volessi collaborare, e mi faceva sapere che aveva i mezzi per farmene pentire. Decisi di piantare i piedi e non collaborare malgrado le pressioni. Una volta pubblicato il libro mi ritraeva come "l'hacker del lato oscuro". Io conclusi che l'autore aveva intenzionalmente incluso affermazioni false e non verificate per vendicarsi del mio rifiuto a collaborare. Rendere il mio personaggio più sinistro e mettendomi in cattiva luce probabilmente aiutò ad aumentare le vendite.
Un produttore di film chiamò con una gran notizia: Hollywood era interessata a fare un film sul sinistro hacker rappresentato in Cyberpunk. Io feci notare come la storia fosse piena d'errori e falsità sul mio conto; il produttore era comunque molto interessato al progetto. Io accettai 5.000 dollari per un'esclusiva di due anni, come acconto di 45.000 se fossero stati in grado di portare a buon fine il progetto.
Quando l'accordo scadde, la compagnia di produzione chiese una proroga di sei mesi. In quel momento io ero impiegato, e avevo poca motivazione nel vedere prodotto un film che mi ritraeva in una luce così cattiva. Rifiutai la proroga. Questo annullò tutti gli accordi per il film, incluso quello di Markoff, che probabilmente si aspettava di fare un mucchio di soldi. Ecco una ragione in più per la quale John Markoff ebbe un atteggiamento vendicativo nei miei confronti.
Più o meno quando Cyberpunk fu pubblicato, Markoff era in contatto via e-mail con l'amico Shimomura. Entrambi erano stranamente interessati nei miei movimenti. Con sorpresa ricevetti un'e-mail che m'informava che avevano saputo che mi trovavo all'Università del Nevada, a Las Vegas, e che avevo accesso alla sala dei computer. Poteva essere che Markoff e Shimomura fossero interessati a scrivere un altro libro su di me? Altrimenti che cosa gli sarebbe importato di sapere che cosa stavo facendo?

>> Markoff all'inseguimento

Facciamo un passo indietro, verso la fine del 1992. Ero vicino alla fine del periodo di libertà vigilata per l'intrusione nel network della Digital Equipment. Nel frattempo, venni a sapere che il governo stava cercando di mettere insieme un altro caso contro di me, questo per aver condotto azioni di contro-spionaggio per scoprire perché erano state messe linee di sorveglianza nei telefoni di una società di Los Angeles. Nella mia ricerca confermai i miei sospetti: gli agenti di sicurezza della Pacific Bell stavano infatti investigano sulla compagnia. Lo era anche un agente specializzato in crimini informatici del dipartimento della contea di Los Angeles.
In questo periodo, i federali si organizzarono con un informatore, e lo mandarono da me per incastrarmi. Sapevano che avevo sempre cercato di essere informato di ogni agenzia che stesse indagando su di me. Quindi fecero in modo che l'informatore diventasse mio amico e mi mettesse a conoscenza del fatto che ero sotto sorveglianza. Inoltre m'informò riguardo a un sistema di computer della Pacific Bell, che mi avrebbe permesso di contro-spiare la sorveglianza. Quando scoprii il piano, velocemente feci girare le carte contro di lui: lo denunciai per le frodi con carte di credito che conduceva mentre stava lavorando per il governo come informatore. Certamente i federali ringrazieranno!
La mia vita cambiò il giorno dell'indipendenza del 1994 quando il teledrin mi svegliò presto la mattina. L'interlocutore mi disse di andare immediatamente a prendere una copia del New York Times. Non ci potevo credere quando vidi che, non solo Markoff aveva scritto un articolo su di me, ma anche che il New York Times lo aveva piazzato in prima pagina. Il primo pensiero fu rivolto alla mia incolumità personale: ora il governo avrebbe aumentato gli sforzi per trovarmi. Fui sollevato dal fatto che, nel tentativo di demonizzarmi, il New York Times aveva usato una foto bruttissima. Non avevo paura di essere riconosciuto, avevano scelto una foto così vecchia che non mi assomigliava per niente. Cominciando a leggere l'articolo mi resi conto che Markoff si stava preparando a scrivere un libro su Kevin Mitnick, come aveva sempre voluto. Non potevo credere che il New York Times accettasse il rischio che comportava stampare le sue illustri falsificazioni. Mi sentii senza speranza. Anche se ero in posizione di contrattaccare, non avevo certo la possibilità di raggiungere lo stesso livello di diffusione del New York Times nel rispondere alle menzogne di Markoff.
Mentre sono d'accordo sul fatto che sono sempre stato stato un rompiballe, non ho mai distrutto informazioni, né ho mai reso note a terzi le informazioni che raccoglievo. Le perdite effettive che le società colpite avevano subìto ammontavano al costo di telefonate che feci a loro spese, i soldi spesi da queste società per riparare i buchi che i miei attacchi avevano rivelato nel loro sistema di sicurezza, e, in alcuni casi, la reinstallazione dei sistemi operativi per paura che avessi fatto modifiche che mi avrebbero successivamente permesso di accedervi. Quelle società avrebbero dovuto affrontare spese molto più alte se le mie attività non avessero eviden-

ziato gli anelli deboli nella catena della loro sicurezza.
Pur avendo causato perdite di denaro le mie azioni non avevano intenzioni così malvagie…
Poi John Markoff cambiò la percezione che il mondo aveva del pericolo che rappresentavo.
L'enorme potere potere di diffamazione posseduto da un giornalista senza etica, che per di più scrive su un giornale così importante, dovrebbe spaventare ognuno di noi. Il prossimo obiettivo potresti essere tu.

>> La sfacchinata

Dopo il mio arresto fui trasportato nella prigione della contea di Smithfield, nel Nord Carolina; qui gli sceriffi ordinarono ai secondini che fossi messo nel "buco", la cella di isolamento. In una settimana l'accusa e i miei avvocati raggiunsero un accordo che non potevo rifiutare. Potevo uscire dall'isolamento a patto che rinunciassi ai miei diritti fondamentali e accettassi: a) di non avere un processo per chiedere la libertà provvisoria; b) nessun processo preliminare; c) niente telefonate, con l'eccezione del mio avvocato e due membri della mia famiglia. Una firma e potevo uscire dall'isolamento. Io firmai.
L'accusa federale giocò tutti gli sporchi trucchi possibili fino a quando fui scarcerato cinque anni dopo. Fui ripetutamente obbligato a rinunciare a diritti fondamentali in modo da essere trattato diversamente da qualsiasi altro recluso. Ma questo era il caso di Kevin Mitnick: non c'erano regole. Non c'era la necessità di rispettare i diritti costituzionali dell'accusato. Il mio caso non riguardava la giustizia, ma la determinazione del governo a vincere a tutti i costi. L'accusa fece stime ampiamente gonfiate dei danni da me causati e del pericolo che rappresentavo. Inoltre, i mass-media avevano colto la palla al balzo, pubblicando affermazioni sensazionalistiche. Era troppo tardi per l'accusa per sminuire. Il governo non si poteva permettere di perdere il caso Mitnick. Il mondo stava guardando. Credo

U.S. Department of Justice
United States Marshals Service

WANTED
BY U.S. MARSHALS

November 1992

che il tribunale si fece influenzare dalle paure generate dai mass-media, giacché molti giornalisti in buona fede avevano riportato i fatti prendendo lo stimato New York Times come fonte.
Apparentemente, il mito generato dai mass-media spaventò anche la polizia. Un documento confidenziale recuperato dal mio avocato mostrava the lo US Marshall Service aveva spedito una circolare avvertendo tutti gli agenti di non rivelare mai a me nessuna informazione personale; altrimenti si sarebbero potuti trovare con le loro "vite elettroniche" cancellate.
La nostra costituzione richiede che una persona sia considerata innocente fino alla sentenza. Questo garantisce a tutti i cittadini il diritto a chiedere la libertà in attesa del processo, atto in cui l'accusato ha la possibilità di essere rappresentato, presentare prove ed esaminare testimoni. Incredibilmente, il governo fu in grado di aggirare tutti questi diritti basandosi sulla falsa isteria generata da giornalisti come John Markoff. Senza precedenti, io fui tenuto in custodia cautelare fino al processo, quattro anni e mezzo dopo. Il rifiuto del giudice di garantirmi un processo per la libertà provvisoria fu combattuto in tribunale fino alla corte suprema. Alla fine, i miei avvocati difensori mi resero noto che avevo stabilito un altro "primato": ero il primo detenuto al quale era stato rifiutato un dibattimento per chiedere la libertà in attesa del processo. Questo significò che il governo non dovette mai assumersi la briga di provare che non c'era forma di libertà provvisoria che non avrebbe pregiudicato la mia partecipazione al processo. Almeno in questa occasione, l'accusa federale non osò affermare che avrei potuto cominciare una guerra nucleare fischiettando in un telefono pubblico, così come altri avvocati avevano detto in un'altra occasione. L'accusa più severa era quella per aver copiato i codici sorgente di diversi telefoni cellulari e di sistemi operativi.
In ogni caso, l'accusa sostenne che io avevo causato a diverse società perdite complessive al di sopra dei 300 milioni di dollari. I dettagli dei valori di queste perdite sono sotto il sigillo della corte, si suppone per proteggere le società coinvolte. I miei avvocati difensori sostengono che l'accusa abbia avviato una pratica per sigillare queste informazioni per coprire la dolosa mistificazione del mio caso. È anche il caso di notare che nessuna delle vittime avesse riportato alcuna perdita al Securities Exchange Commission (l'organo di controllo della borsa americana, Ndr), così come la legge richiede. O molte multinazionali violarono la legge federale ingannando la SEC, gli azionisti e gli analisti, o le perdite attribuite al mio hacking erano, di fatto, troppo lievi per essere riportate.
Nel suo libro "Il gioco del fuggitivo" Jonathan Littman racconta che una settimana dopo la pubblicazione di quella prima pagina del New York Times, l'agente di Markoff aveva raggiunto un accordo con la casa editrice Walt Disney Hyperion per un libro sulla campagna poliziesca per catturarmi. L'antici-

po era da stimarsi nell'ordine dei 750.000 dollari. Secondo Littman, ci sarebbe stato anche un film Hollywoodiano, la Miramax avrebbe anticipato 200.000 di dollari per l'esclusiva, e ne avrebbe saldati 650.000 nel momento in cui si cominciasse a filmare. Un fonte confidenziale mi ha recentemente fatto sapere che, in effetti, l'accordo preso da Markoff era maggiore di quello che Littman aveva stimato.
Quindi John Markoff si è beccato più o meno un milione di dollari, e io 5 anni di galera.

>> Cosa dicono gli altri

Un libro che esamina gli aspetti legali del mi caso è stato scritto da una persona che aveva precedentemente lavorato come pubblico ministero nell'ufficio del procuratore distrettuale di Los Angeles: un collega degli avvocati che avevano formato l'accusa nel mio caso. In questo libro, "Crimini informatici spettacolari", Buck Bloombecker scrive: "mi addolora di dover scrivere a proposito dei miei passati colleghi con parole di disistima… Sono perseguitato dal ricordo dell'ammissione di James Asperger, assistente del procuratore distrettuale, secondo il quale la maggior parte delle argomentazioni utilizzate per tenere Mitnick dietro le sbarre fu basata su dicerie che non avevano senso". E poi continua: "Era già abbastanza brutto che i capi d'accusa portati in aula fossero stati disseminati a milioni di lettori da quotidiani di tutte le parti della nazione. È ancora peggio che queste supposizioni costituirono, per la maggior parte, la base per mantenere Mitnick dietro le sbarre senza la possibilità di chiedere la libertà provvisoria".
Poi continua per un po' parlando dei livelli etici che un pubblico ministero dovrebbe seguire come regole di vita, e infine scrive: "il caso Mitnick suggerisce che le false affermazioni utilizzate per tenerlo in custodia cautelare, pregiudicarono in seguito le valutazioni della corte, quando emise la sentenza".
Nel suo articolo apparso su Forbes nel 1999, Adam L. Penenberg descrive eloquentemente la mia situazione nel seguente modo: "I crimini di Mitnick furono curiosamente innocui. Entrò in computer aziendali, ma non c'è prova che indichi che distrusse dati. O che abbia venduto quello che copiò. Sì, rubò software, ma facendolo lo lasciò dov'era". L'articolo disse che il mio crimine fu di "cacciare il naso nei costosi sistemi di sicurezza dei computer utilizzati dalle multinazionali". Nel libro "Il gioco del fuggitivo", l'autore Jonathan Littman dice: "Il governo poteva capire l'avidità. Ma un hacker che bramasse il potere in se stesso, era qualcosa che non potevano concepire".
In un altro punto dello stesso libro, Littman scrive: "Il pubblico ministero James Sanders, parlando con il giudice Pfaelzer, ammise che il danno causato alla DEC non fu di 4 milioni di dollari, come i titoli dei giornali riportarono, ma di 160.000. Anche questa cifra non costituiva il reale danno causato da Mitnick, ma la spesa approssimativa sostenuta da DEC per riparare i buchi nella sicurezza resi evidenti dall'incursione, ma presenti già da prima. Il governo ammise che non aveva prove per le dichiarazioni che avevano contribuito a mantenere Mitnick in prigione e in cella d'isolamento. Non c'era prova che Mitnick avesse mai compromesso la sicurezza della NSA. Non c'era prova che Mitnick avesse mai inviato un falso comunicato di stampa a nome della Security Pacific Bank. Non c'era prova che Mitnick avesse mai modificato il rapporto di credito di un giudice. Ma il giudice, forse influenzato dal terrificante resoconto dei mass-media, rifiutò una possibilità d'accordo e condannò Mitnick a una pena addirittura maggiore di quella voluta dal pubblico ministero.
Durante gli anni spesi da hacker dilettante, guadagnai una non voluta notorietà, fui menzionato in molti articoli di giornali e quattro libri furono scritti su di me. Il libro diffamatorio, scritto da Markoff e Shimomura, fu trasformato in un film chiamato Takedown. Quando il copione raggiunse Internet, molti dei miei fan organizzarono manifestazioni di fronte alla Miramax, per attrarre l'attenzione dell'opinione pubblica sulla inaccurata e falsa caratterizzazione del mio personaggio. Senza l'aiuto di molte buone e generose persone, la casa cinematografica mi avrebbe certamente rappresentato come l'Hannibal Lecter del cyberspazio. Sotto le pressioni dei miei fan, la casa di produzione si accordò per sistemare il caso in maniera privata per evitare che io cominciassi un'azione legale contro di loro.

>> Considerazioni finali

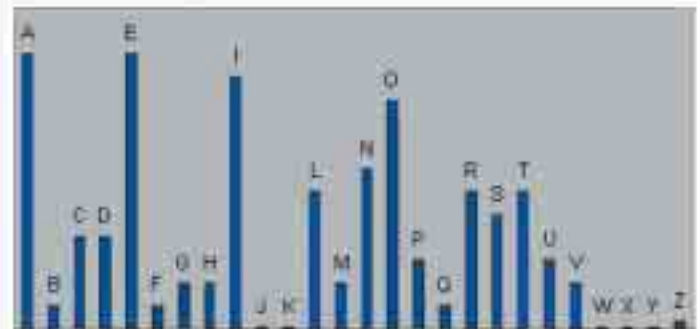
Nonostante la descrizione diffamatrice e offensiva che John Markoff fece di me, i miei crimini erano semplici intrusioni in computer e telefonate gratis. Io ho ammesso che le mie azioni erano illegali, e che ho invaso la privacy di altri. Ma suggerire senza giustificazione, ragione o prova, come Markoff fece nei suoi articoli, che avessi sottratto soldi o proprietà con il mezzo della truffa via computer o via cavo, è semplicemente falso, e non è supportato da nessuna prova.
Le mie malefatte erano motivate da curiosità: volevo sapere tutto quello che c'era da sapere sulla maniera in cui i network telefonici funzionavano, e su tutti i particolari dei sistemi di sicurezza. Dal ragazzino che amava fare giochi di prestigio, sono diventato essere l'hacker più famoso del mondo, temuto da società e governi.
Mentre rifletto sulla mia vita di questi ultimi trenta anni, devo ammettere di aver preso molte decisioni stupide, guidato dalla mia curiosità, dal desiderio di imparare la tecnologia e da una sorta di sfida intellettuale.
Ora sono una persona cambiata. Utilizzo i miei talenti e le profonde conoscenze sulla sicurezza informatica e le tecniche dell'ingegneria sociale per aiutare governi, società e individui a prevenire, scoprire risolvere gli attacchi alla sicurezza delle informazioni.
Questo libro è un modo in più per utilizzare la mia esperienza per aiutare altri a sopraffare lo sforzo dei ladri d'informazione del mondo. Io credo che troverete le storie divertenti, educative e illuminanti.

Kevin Mitnick

...quando la crittanalisi era in vantaggio

Partiamo con il formulare uno dei principi della crittografia, la legge di Kerckhoffs (1883): **"La sicurezza di un crittosistema non dipende dal tenere nascosto l'algoritmo ma dipende dal tener nascosta la chiave"**
Vediamo quindi se il metodo di Vigenere, a cui abbiamo accennato nel n. 11 e 12, può essere ritenuto sicuro in base a tale principio.
Prendiamo quindi in esame il seguente testo che sappiamo essere codificato con il metodo di Vigenere, ma non conosciamo la chiave, e vediamo passo dopo passo come dobbiamo muoverci per decifrare il testo. Apparentemente sembrerebbe una impresa impossibile e così lo è stato per molto tempo finchè non è arrivato un ufficiale pensionato dell'esercito prussiano, Kasiski che nel lontano 1863 mandò in soffitta la codifica alla Vigenere.

```
WBSKMUASKMULGLTZVGUKOAHGIKYSNBJLBRB
GYSUHSLWDFKACVHOKSSMUKOCTYPGCBVVGKT
KZGWKKBBEXZVRGXLMWUTILDWKJLQAYXHFWF
KZGSZMPQJBZAOLBIVBDTZLQFBIHRAOONSFX
XLWDFKACVHAZODTZLQFBIHRATZAOUVUIOKT
ZHGMERHFAIKAWRBUUSVBGSQMGONFMIVPRAE
KAHWKKHZDBTASJGUKSDFKZGSZMPCUBLYOLH
```

Nel testo cifrato si possono vedere delle stringhe evidenziate di vario colore; infatti il primo passo del metodo di Kasiski è nell'individuare la ripetizione di alcune stringhe all'interno del testo crittato e di segnarne la distanza.
Quindi da questa prima analisi abbiamo trovato che:
La stringa SKMU (verde) si ripete a distanza di 5 (ossia le due "S" sono separate da 4 lettere)
La stringa DFKACV (rossa) si ripete a distanza di 100 (ossia le due "D" sono separate da 99 lettere)
La stringa FKZGSZMP (arancione) si ripete a distanza di 125
La stringa DTZLQFBIHRA (blu) si ripete a distanza di 30
Conviene prendere in esame stringhe ripetute la cui estensione sia almeno di 4 lettere, perché altrimenti con lunghezze inferiori si potrebbero fare ragionamenti erronei sulla lunghezza della chiave.
Adesso dobbiamo per ogni distanza scrivere tutti i numeri interi (perché la chiave sarà costituita per forza da un numero intero) che sono suoi divisori. I divisori sono tutti i numeri N che verificano la seguente equazione:

Distanza (mod) N = 0

Quindi i divisori per le varie stringhe sono:

```
SKMU         1  5
DFKACV       1  2  4  5  1  20  25  50  100
FKZGSZMP      1  2  3  5  6  10  15  30
DTZLQFBIHRA  1  5  25  125
```

I divisori comuni a tutte le stringhe sono 1 e 5.
Quindi stando così le cose la nostra analisi porta a dire che la lunghezza della chiave o è 1 (il che vorrebbe dire che ci troveremmo di fronte ad una cifratura alla Cesare, che è quindi scardinabile con un banalissimo Brute Force con soli 26 tentativi) oppure è 5.
Quindi la lunghezza della chiave è 5 e già abbiamo fatto un notevole passo in avanti; uno dei punti più critici di tutto il procedimento è stato fatto.

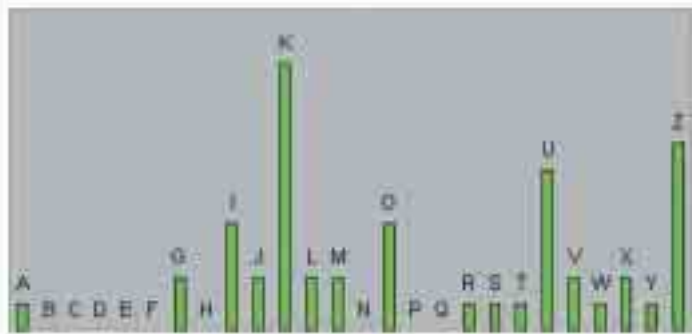
>> Procediamo con la decifratura

Possiamo quindi dividere il testo in gruppi di cinque lettere. Tutte le prime lettere di ogni gruppo sono state codificate con lo stesso alfabeto cifrante; ossia tutte le lettere verdi sono state cifrate con lo stesso alfabeto di Cesare, di cui però non conosciamo la chiave di traslazione. Lo stesso per tutte le lettere rosse e via via per le altre.
Quindi adesso il problema è diventato trovare 5 alfabeti di Cesare cifranti, perché 5 è la lunghezza della chiave.
Il messaggio così separato assume la forma:

WBSKMUASKMULGLTZVGUKOAHGIKYSNBJLBRB
GYSUHSLWDFKACVHOKSSMUKOCTYPGCBVVGKT
KZGWKKBBEXZVRGXLMWUTILDWKJLQAYXHFWF
KZGSZMPQJBZAOLBIVBDTZLQFBIHRAOONSFX
XLWDFKACVHAZODTZLQFBIHRATZAOUVUIOKT
ZHGMERHFAIKAWRBUUSVBGSQMGONFMIVPRAE
KAHWKKHZDBTASJGUKSDFKZGSZMPCUBLYOLH

Per cercare di capire a quale lettera italiana corrisponde ogni lettera cifrata, ci si baserà sul metodo delle frequenze. In ogni lingua, per qualsiasi testo sufficientemente lungo, certe lettere compaiono più di altre. Analizzando le frequenze medie dell'italiano, e quelle delle singole lettere che compaiono nel testo cifrato (vedere le figure in queste pagine), possiamo così stabilire una relazione.

>> Lettere verdi

Una analisi delle frequenze condotta su tale raggruppamento di lettere dà il risultato che si vede nella figura. Come si può notare, in italiano è scarsa la presenza delle lettere W X Y Z, mentre per le lettere verdi vi è una scarsa frequenza delle lettere B C D E F; quindi sembrerebbe che le lettere W X Y Z siano state cifrate con le lettere B C D E F.

Si noti che abbiamo una incertezza perché l'ampiezza di questo avvallamento (scarsa frequenza di lettere) è diversa nei 2 grafici. Ma vediamo cosa altro possiamo leggere dalla comparazione dei due istogrammi. In italiano abbiamo la presenza di picchi in corrispondenza delle lettere A E I O, mentre per le lettere verdi abbiamo dei picchi in K U Z.
Inoltre la mancanza delle lettere J K in italiano sembrerebbe esserci anche nelle lettere verdi per la P Q.
In conclusione da questa analisi ad "occhio" abbiamo ipotizzato le seguenti corrispondenze:

Italiano	**Testo cifrato**
W X Y Z	B C D E F
A E I O	K U Z
J K	P Q

Allora in base a queste considerazioni possiamo dedurre che l'alfabeto chiaro

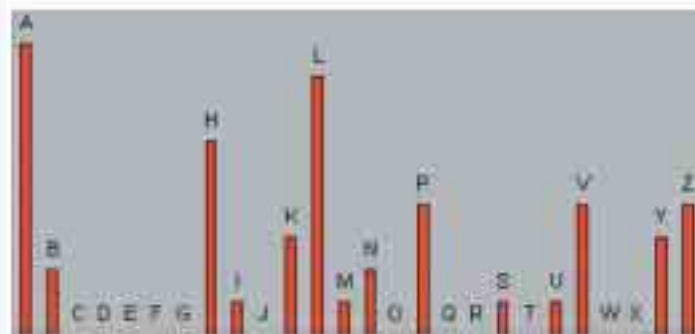
ABCDEFGHIJKLMNOPQRSTUVWXYZ

È stato cifrato nella seguente maniera

GHIJKLMNOPQRSTUVWXYZABCDEF

L'alfabeto cifrante è scritto in modo da verificare molte delle considerazioni ricavate ad "occhio"
Infatti abbiamo la corrispondenza fra J e P; K e Q; E e K; O e U; W e C; X e D; Y ed E; Z e F.
Da tale discorso deduciamo che la prima lettera della chiave è la prima lettera dell'alfabeto cifrante ossia G.

>> Lettere rosse

Prendiamo ora come riferimento la figura che mostra il risultato dell'analisi delle frequenza con cui compaiono le varie lettere tra i caratteri in rosso.

Da un'analisi "a occhio" questa volta sembrerebbe che:

Italiano	**Testo cifrato**
W X Y Z	C D E F G
A E I O	A H L
J K	Q R oppure W X

In base a queste considerazioni possiamo dedurre che l'alfabeto chiaro:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

È stato cifrato nella seguente maniera:

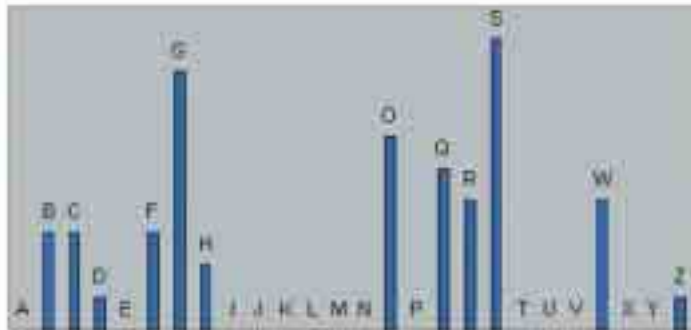
HIJKLMNOPQRSTUVWXYZABCDEFG

In tal modo abbiamo la corrispondenza fra J e Q; K e R; E e L; A e H; W e D; X e E; Y e F; Z e G.
Quindi la seconda lettera della chiave cifrante è H.

>> Lettere celesti

Una analisi delle frequenze condotta su tale raggruppamento di lettere da il risultato che si può osservare in figura.
In questo caso, osservando la frequenza delle lettere si è

portati a pensare che la corrispondenza sia questa:

Italiano	**Testo cifrato**
W X Y Z	I J K L M N
A E I O	G O S

J K T U V oppure X Y
Possiamo dedurre che l'alfabeto chiaro
ABCDEFGHIJKLMNOPQRSTUVWXYZ

È stato cifrato nella seguente maniera
OPQRSTUVWXYZABCDEFGHIJKLMN

Infatti abbiamo la corrispondenza fra J e X; K e Y; E e S; A e O; W e K; X e L; Y e M; Z e N.
Quindi la terza lettera della chiave cifrante è O.

>> Trovare il resto

Per adesso la chiave che abbiamo trovato è GHO**.
Mmmm….. Non mi sembra avere molto senso; controlliamo se stiamo facendo bene.
Abbiamo individuato gli alfabeti cifranti delle lettere verdi, rosse e celesti, quindi proviamo a decifrare questi gruppi di lettere e vediamo se otteniamo qualcosa di decente e comprensibile:
Questo è il testo parzialmente decrittato:

```
QUEKMOTEKMOESLTTOSUKITTGIERENBDENRB
AREUHMEIDFETOVHIDESMODACTSISCBPOSKT
ESSWKEUNEXTODGXFFIUTCEPWKDECAYRARWF
ESSSZGICJBTTALBCONDTTECFBCADAOIGEFX
REIDFETOVHUSADTTECFBCADATTTAUVOBAKT
TASMELARAIETIRBONEVBALCMGIGRMIPIDAE
ETTWKEALDBNTEJGODEDFESSSZGIOUBFRALH
```

Adesso ragioniamo sugli elementi a disposizione e vediamo se possiamo intuire l'alfabeto cifrante delle lettere arancioni e nere.
Vediamo le prime lettere QUEKMOTEKMO che vi viene in mente?
Potrebbe essere QUESTOTESTO? Ossia che la S sia stata cifrata in K e la T in M?

Kasiski sul computer

La fase più difficile da implementare al calcolatore sarebbe quella di far riconoscere la ripetizione di stringhe significative all'interno del testo crittato. Utilità di tale passo è solamente quella di determinare la lunghezza della chiave, e quindi può essere bypassato imponendo al programma di provare una deciifratura variando di volta in volta la lunghezza della chiave, fino a quando non esce fuori un testo chiaro comprensibile e questo molto spesso è accompagnato anche dall'individuazione di una chiave anch'essa comprensibile.
La comparazione fra le tabelle delle frequenze che noi abbiamo condotto "a occhio", in realtà viene spesso risolta matematicamente analizzando, in maniera più o meno complessa, le differenze di altezza fra le varie colonne.

È una ipotesi di lavoro del tutto plausibile!
Per le lettere arancioni l'ipotesi di lavoro è:

Alfabeto chiaro:
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Alfabeto cifrato:
STUVWXYZABCDEFGHIJKLMNOPQR

Costruito per avere la corrispondenza fra S e K.
Quindi la quarta lettera della chiave è S.
Analogamente per le lettere nere:

Alfabeto chiaro:
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Alfabeto cifrato:
TUVWXYZABCDEFGHIJKLMNOPQRS

Costruito per avere la corrispondenza fra T e M.
Quindi la quarta lettera della chiave è T.
Dal nostro ragionamento abbiamo ottenuto finalmente la chiave: **GHOST**.
Tale chiave sembra avere un senso e allora applichiamola al testo cifrato con il metodo di Vigenere, e otteniamo così alla fine il testo in chiaro:

```
QUESTOTESTOESTATOSCRITTOPEREVIDENZI
ARECOMEILMETODOIDEATODAKASISKIPOSSA
ESSEREUNMETODOEFFICACEPERDECIFRAREM
ESSAGGICRITTATICONLATECNICADIVIGENE
REILMETODOUSALATECNICADIATTACCOBASA
TASULLARIPETIZIONEDIALCUNIGRUPPIDIL
ETTEREALLINTERNODELMESSAGGIOCIFRATO
```

Naturalmente non sempre l'analisi con il metodo di Kasiski è così semplice e diretta, e spesso le ipotesi di lavoro sono errate e bisogna quindi tornare indietro e provarne altre. Soprattutto, non sempre si ha a che fare con un sistema crittografico così semplice da scardinare, ma è importante conoscere i principi di base della crittanalisi.

>>——Robin——>

IDENTIKIT DI UN PENNUTO

Per descrivere Linux, bisogna parlare di multitasking, multiutenza, portabilità, compatibilità Posix... Ma cosa significano questi termini, e perché sono tanto importanti?

Definire cosa sia un sistema operativo è impresa assai ardua, e l'esistenza di moltissimi sistemi spesso profondamente differenti tra loro non aiuta certo nel compito. Possiamo comunque pensare al sistema operativo come a **un entità software formata da diverse componenti: il kernel, la shell e i programmi "di servizio"**. Il kernel (o nucleo) in particolare è quella componente che si incarica della gestione dei diversi dispositivi hardware (periferiche di I/O, CPU, memorie...) e dell'allocazione di queste stesse risorse ai diversi programmi che le richiedono. La shell (sia essa la tradizionale "riga di comando" o una più moderna interfaccia grafica) è invece un particolare programma che, ponendosi a metà strada tra il kernel e l'utente, consente all'utente stesso di accedere al sistema e ai suoi servizi. Come abbiamo già visto in passato, **con il termine Linux ci si riferisce proprio al kernel e non tanto al sistema operativo completo** di shell e tools di amministrazione (**che è invece chiamato GNU/Linux**).

Su un computer con Linux possono lavorare contemporaneamente svariati utenti, utilizzando un altro sistema Posix oppure da terminale a linea di comando.

>> La conoscenza è potere!

Ogni sistema operativo e, in particolare, ogni kernel presenta determinate caratteristiche; se Linux è oggi adottato in moltissimi ambiti e per svolgere le funzioni più disparate è proprio perchè, oltre ad essere diffuso liberamente, **negli anni ha spesso raggiunto e superato gli altri sistemi in quanto a prestazioni, funzionalità ed affidabilità**. Ma vediamo di analizzare con ordine le principali caratteristiche della creatura di Mr. Torvalds.

>> Kernel monolitico e modulare

Esistono essenzialmente due tipologie radicalmente differenti di kernel: "monolitico" e "microkernel". Senza approfondire ulteriormente l'argomento, basti sapere che ogni approccio presenta punti di forza ma anche diversi limiti e Torvalds, quando iniziò a lavorare a Linux, **optò per un kernel monolitico principalmente perchè meno complesso da implementare**; quest'ultimo in pratica altri non è infatti che un unico, grande, file che svolge tutte le funzioni.

La scelta di Linus fu motivo di aspre discussioni tra Andrew Tanenbaum, creatore di Minix (che è un microkernel), e lo stesso Linus ma alla fine, come è logico presupporre, non si giunse ad una vera conclusione poiché entrambi difesero la propria posizione pur sapendo che non era, in assoluto, migliore dell'altra. Tuttavia l'aver optato per un kernel monolitico ha fatto sì che sin dall'inizio **i driver dei diversi dispositivi venissero inclusi direttamente all'interno del kernel**; è evidente quindi come questo abbia comportato un aumento spaventoso delle dimensioni del kernel stesso, "costringendo" a una revisione della struttura di base di Linux.

A partire dal kernel 2.0 è stato perciò introdotto l'utilizzo dei moduli caricabili per i driver e per altre componenti quali i file system. I moduli infatti, pur essendo parte integrante del kernel, possono essere compilati separatamente e cari-

cati solo all'occorrenza. È importante notare come, una volta caricati, i moduli diventino parte integrante del kernel e pertanto **in grado di far danni come se fossero stati compilati direttamente nel kernel**; tuttavia, come ha ammesso lo stesso Linus, un sistema il più modulare possibile è quanto di meglio ci possa essere per un modello di sviluppo open source.

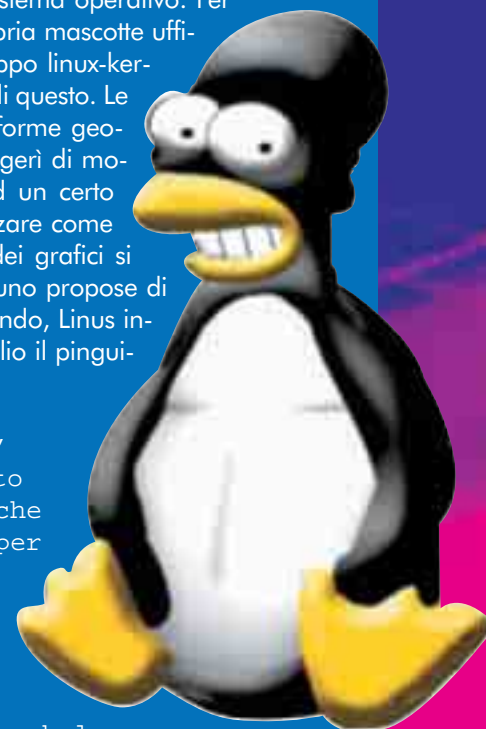
>> Multitasking

Linux è in grado di eseguire diverse attività nello stesso momento; mentre per esempio un programma avviato dall'utente è in esecuzione, l'elaboratore è in grado di leggere o scrivere dati su disco e gestire la stampa di un documento.
Infatti, nonostante la CPU sia in grado di eseguire un solo processo per volta, un sistema di questo tipo (detto anche multiprogrammato) gestisce i vari programmi in coda continuando ad alternarli. In questo modo **la CPU continua rapidissimamente a passare da un processo all'altro dando all'utente l'illusione che più programmi siano contemporaneamente in esecuzione**.
Inoltre Linux, supportando macchine multiprocessore, è in grado anche di fornire un vero parallelismo hardware (cioè non solo apparente) nell'esecuzione dei processi.

>> Multiutenza

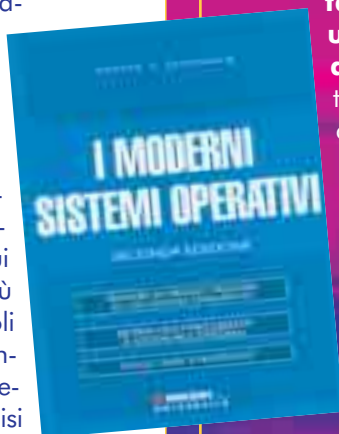
Un sistema Linux può essere utilizzato contemporaneamente da più utenti, ciascuno connesso alla macchina dal proprio terminale. In particolare **a ogni utente registrato è associato un profilo (account) e questi può accedere so-**

Un pinguino di nome Tux

Quel simpatico e omnipresente pinguino che fa capolino ormai su ogni sito dedicato a Linux e che riempie le pagine della nostra rivista è, come avrete probabilmente già intuito, la mascotte ufficiale di questo sistema operativo. Per lungo tempo Linux non poté però vantare una propria mascotte ufficiale finché nel 1996, sulla lista principale di sviluppo linux-kernel, diverse persone iniziarono a discutere proprio di questo. Le idee non mancarono: molti proposero animali o forme geometriche più o meno astruse mentre qualcuno suggerì di modificare in chiave ironica loghi di altri sistemi. Ad un certo punto tuttavia Linus Torvalds dichiarò di voler utilizzare come logo un pinguino; a questo punto tutti gli sforzi dei grafici si concentrarono su questo animale e quando qualcuno propose di realizzare un pinguino nell'atto di sorreggere il mondo, Linus intervenne con una lunga mail descrivendo in dettaglio il pinguino che tanto avrebbe voluto vedere...

```
"[…] Quando pensate ad un 'pinguino'
dovreste immaginarne uno ben pasciuto
(non GRASSO, ma si dovrebbe vedere che
è seduto perchè ha mangiato troppo per
poter restare in piedi) seduto e
soddisfatto perchè ha appena dige-
rito. Inoltre dovrebbe essere sor-
ridente e avere un'aria beata - il
mondo dopotutto è un bel posto dove
stare quando avete appena mangiato un bel
po di pesce fresco e sentite che un ruttino sta per
salire. […]"
```

Lo stesso Linus spiegò inoltre che voleva un qualcosa di semplice come logo ufficiale; questo avrebbe anche permesso a tutti di utilizzarlo per creare facilmente versioni "modificate" da inserire nelle pagine Web, sulle copertine dei CD, sulle magliette... Passarono pochi giorni quando una nuova mail di Linus annunciò il vincitore del "Linux-Logo Contest": Larry Ewing. Ancora oggi sul sito Internet di Larry (http://www.isc.tamu.edu/~lewing/linux/) sono presenti le immagini originali e una spiegazione di come lo stesso sia riuscito, utilizzando il programma di grafica GIMP (The GNU Image Manipulation Program), a creare il famoso pinguino. Inoltre l'autore permise da subito a chiunque di utilizzare o modificare il pinguino da lui creato; in questo modo ben presto le pagine Web iniziarono a pullulare di pinguini impegnati a leggere libri o giornali, giocare (o litigare) con il diavoletto di FreeBSD, abbracciare modem o perifiche varie, spegnere candeline, saltare etc...
Come è lecito supporre, al nostro amato pinguino venne ovviamente dato anche un nome: Tux. Tuttavia, sebbene in inglese 'tuxedo' significhi 'frac, abito da sera' (capo d'abbigliamento che richiama un po' i colori e la forma del pinguino...), il nome della mascotte di Linux ha anche un altro significato: Tux è l'acronimo di (T)orvalds (U)ni(X). Giusto nel caso vi foste dimenticati chi è l'autore di Linux.... :)

UN LIBRO ILLUMINANTE

Parlando di Linux e di Unix siamo più volte incappati in un personaggio molto particolare: Andrew S. Tanenbaum. Questi infatti non solo è il creatore di Minix (da cui "discende" anche Linux) ma anche l'autore de I Moderni Sistemi Operativi. Professore all'università di Amsterdam, Tanenbaum ha da sempre pensato il suo volume, considerato 'la Bibbia' dei SO, per un corso universitario e questo ha fatto sì che oggi sia utilizzato con successo nelle università di mezzo mondo. In particolare la seconda edizione, di recente pubblicata in Italia da Jackson Libri (51.50 Euro), si focalizza principalmente sui sistemi operativi a singolo processore e integra nuovi capitoli sulla sicurezza o sui sistemi operativi oggi più diffusi. I primi sei capitoli contengono le nozioni fondamentali sui sistemi operativi, iniziando dall'analisi della struttura di un SO e dalle chiamate di sistema, passando per i processi e i thread, le situazioni di stallo (deadlock) o la gestione della memoria e concludendo con un'analisi sulle modalità di gestione dell'I/O e del FileSystem. Nella seconda parte, insieme ad un analisi dei sistemi multiprocessore e distribuiti, trovano spazio due nuovi capitoli sui sistemi operativi multimediali e sulla sicurezza (crittografia, autenticazione, analisi degli attacchi dall'interno e dall'esterno del sistema e meccanismi di protezione). Concludono il tutto due dettagliati casi di studio dedicati rispettivamente a Windows 2000 e Unix (con particolare attenzione a Linux) e un capitolo dedicato alla progettazione dei sistemi. Come ha ammesso lo stesso Tanenbaum, gli ultimi capitoli sono decisamente più interessanti dei primi ma si "dovranno mangiare i broccoli prima di poter gustare la torta al cioccolato"; pertanto buona lettura e... buon appetito

lo a determinate risorse del sistema o eseguire determinate operazioni in base ai privilegi che impostati dall'amministratore. Un utente particolare è **root: questi è infatti l'amministratore dell'intero sistema**; tuttavia proprio per questo motivo il suo utilizzo è da limitare al massimo (un errore compiuto come root può avere conseguenze disastrose!).

>> Portabilità

Per "portabilità" di un sistema operativo si intende **la capacità di quest'ultimo di funzionare su piattaforme differenti con un numero trascurabile di modifiche al codice**; tanto minori sono le modifiche da apportare, tanto più questo sistema è portabile. Tradizionalmente i kernel monolitici, a differenza dei microkernel, non sono mai stati molto portabili ma Linux, in questo caso, fa eccezione. Il fatto di essere stato scritto per lo più in C e solo in minima parte in linguaggio Assembly ha infatti permesso di far funzionare Linux su moltissimo hardware; secondo solo a NetBSD, Linux oggi supporta i processori **x86 (286 inclusi!) a 32 e 64 bit, Digital Alpha, SPARC e UltraSPARC, MIPS, ARM, Macintosh, PowerPC, s390** e si è diffuso anche in settori tradizionalmente off-limits quali il mondo delle applicazioni embedded, i palmari e le console (**dalla PlayStation alla X-Box passando per la Sega Dreamcast**).

>> Scalabilità

La scalabilità di un sistema operativo è la sua capacità di gestire un sempre maggior numero di risorse hardware (numero di processori, quantità di memoria, hard disk...). In pratica il sistema deve essere in grado di gestire le risorse che via via si aggiungono aumentando le prestazioni in maniera proporzionale; esiste tuttavia un punto di rottura oltre il quale le prestazioni invece di aumentare diminuiscono e il tutto diventa inaffidabile.
Il fatto che molti tra i principali centri di calcolo e di analisi e persino alcuni dei più veloci computer al mondo utilizzino Linux, dimostra come questo sistema operativo sia in grado di fornire risposte soddisfacenti anche in situazioni limite.

>> Posix-Compatibile

Linux è basato sullo standard POSIX (International Standard 9945-1), comune un po' a tutto il mondo degli Unix; in altre parole, **Linux è compatibile con Unix a livello di chiamate di sistema**.
Questo significa che una gran parte dei programmi originariamente scritti per altri Unix possono essere ricompilati sotto Linux con poche modifiche e, allo stesso modo, **il software pensato per Linux può facilmente essere riutilizzato su altre versioni *nix**.

>> Scoprite il resto!

In aggiunta a questo, Linux offre una protezione della memoria in modo da evitare che il crash di un singolo programma mandi in bomba l'intero sistema, emula a livello kernel le istruzioni FPU su sistemi senza coprocessore matematico, gestisce la memoria virtuale attraverso la paginazione su disco (grazie ad apposito aree di swap), supporta nativamente moltissimi filesystems tra cui NTFS, FAT16 e FAT32, BeFS o HFS e dispone di moderni journaledFS tra cui Ext3, ReiserFS, XFS...
Ovviamente le caratteristiche di Linux non si esauriscono a questa breve carrellata ma per ora lascio a voi il compito di scoprire quanti altri segreti questo sistema operativo ancora nasconda. I punti di partenza sono i soliti: i siti www.linux.org e www.kernel.org

lele - www.altos.tk

QUANDO L'HARDWARE È UN PO' SOFT

Non sono solo i server e i sistemi operativi a offrire il fianco ad attacchi di vario tipo: anche i router hardware infatti...

Un **gateway** è un punto di accesso di una rete verso un'altra rete. Se per esempio volete connettere la vostra rete domestica a Internet, qualunque pacchetto debba dirigersi verso un indirizzo esterno al classico 192.168.xxx.xxx della configurazione interna di rete, dovrà passare dal gateway che voi avrete impostato. I gateway sono classificati secondo il modello OSI che definisce come livello 1, fisico, i ripetitori; livello 2, data-link, i bridge, e livello 3, rete, i router. Noi tratteremo principalmente quest'ultima categoria andando a spulciare nella rete le ultime scoperte a riguardo, **analizzando i problemi legati all'uso di tali dispositivi, le tecniche note di attacco e le soluzioni proposte dai vari produttori da adottare per difendersi**.

Facciamo una premessa brevissima tanto per ricordare come funziona un router. Esso, sia che debba unire reti locali, sia che debba unire reti geografiche, basa il suo funzionamento sulla **tabella di routing**. Essa viene creata partendo dalle intestazioni del protocollo e, in base ad essa, proietta sulla rete i vari pacchetti seguendo regole precise e decise a monte dall'amministratore. I pacchetti che arrivano al router vengono immagazzinati in una coda in modo tale da poter essere analizzati uno per uno e prendere la giusta decisione a riguardo, senza il rischio di perdere neppure un dato. Secondo le politiche create nel router, un pacchetto può essere diretto in una direzione piuttosto che in un'altra oppure può essere scartato se non conforme agli standard impostati. Tutte queste regole vanno sotto il nome di **politiche di filtraggio e sono gestite direttamente dall'amministratore di sistema**. Attualmente si considera che **circa l'80-90% dei router presenti sul mercato siano affetti, potenzialmente, da qualche baco che può essere sfruttato per guadagnare i privilegi di amministratore** del router e quindi per poter cambiare le sue configurazioni.

>> Ascend – Lucent

Questi prodotti, reperibili su internet all'indirizzo www.lucent.com, fanno parte di un'offerta molto vasta che va da router impiegati in reti geografiche fino ai domestici o reti comunque piccole.

I rischi documentati che riguardano queste apparecchiature sono fondamentalmente quattro, e più precisamente:

1 **pipeline password congestion**: attaccando il router con continue richieste di telnet si riesce a saturare le sue risorse in modo tale che non reagisca più in seguito a richieste legittime, bloccando così ogni tentativo di accesso esterno di tipo telnet. La serie interessata è quella della famiglia Ascend Pipeline.

2 **Ascend MAX**: la MAX è una famiglia di router che sono sensibili ad un attacco telnet portato sulla porta 150, che tramite l'invio di pacchetti TCP con offset diverso da zero, riescono a resettare e riavviare la macchina in modo remoto. La serie interessata è quella Ascend MAX ed il tool per effettuare tali attacchi si può reperire in rete e va sotto il nome di TCPoffset.c

3 **attacco distorted UDP**: alcuni router Ascend hanno un difetto

GATEWAY, ROUTER E LORO PUNTI DEBOLI

intrinseco nel loro sistema operativo e che permette di bloccarli, spendendo determinati pacchetti di tipo UDP. Il difetto si può riassumere nel seguente modo: mandando un pacchetto UDP come messaggio broadcast sulla porta 9 del router, esso risponde con un altro pacchetto UDP che contiene anche il nome del router stesso. Mandando quindi un ulteriore pacchetto UDP a questa porta si riesce a provocare il blocco del sistema. Questo baco è facilmente esplorabile con in TigerBreach, uno dei tanti tool contenuti nel kit TigerSuite.

4 attacco TCP offset: i server per terminali Ascend possono essere bloccati tramite l'invio di un pacchetto con offset diverso da zero. Il file ascend.c può essere utilizzato a tale scopo.

>> 3Com

Una delle più grandi società a livello mondiale di produzione di tali hardware. Offre prodotti per tutte le necessità, dalla famiglia all'impresa. È rintracciabile su internet all'indirizzo www.3com.com.

I rischi documentati per questa marca di prodotti sono:

1 HiPer ARC DoS: i prodotti della serie HiPer ARC sono vulnerabili ad attacchi di tipo denial of service e risultano in un blocco totale del sistema. Il listato Nestea.c può essere utilizzato dagli amministratori per controllare la sicurezza dei propri sistemi. I prodotti interessati sono quelli con versione 4.1.11

2 HiPer ARC card login: è un attacco che porta come risultato un accesso non autorizzato alla scheda. Il baco sta nell'account standard adm ed i sistemi potenzialmente craccabili con questa tecnica sono quelli della serie 4.1.x. il baco è un problema molto serio in quanto, al primo accesso alla macchina come adm senza password, il proprietario creerà un proprio account prevosto di login e password. Dopo aver salvato i dati l'account adm senza password rimane attivo e non può più essere cancellato.

3 master key: su internet si possono facilmente reperire della master key, ovvero degli accoppiamenti username/password che danno accesso al router. I modelli interessati da questo bug sono: CoreBuilder 2500 — 3500 — 6000 — 7000 ed i SuperStack II 2200 — 2700 — 3500 — 9300. Alcuni esempi, giusto per citarne un paio dei più noti sono tech/tech e debug/synnet per i CoreBuilder.

>> Cabletron – Enterasys

Su www.enterasys.com si può trovare l'offerta di questa casa produttrice di hardware. Sono prodotti rivolti soprattutto alle aziende ed alle reti di grandi dimensioni, lavorando principalmente sopra il Gigabit di banda.
I rischi documentati più importanti sono riassumibili come:

1 CPU Jamming: è un attacco di tipo flooding al quale sono vulnerabili i prodotti della serie SmartSwitch router. Il risultato dell'attacco è un'interferenza nell'elaborazione delle tabelle ed un rallentamento del sistema. Si sfrutta, per tale scopo, l'invio di numerosi pacchetti caratterizzati da IP del tipo 0.0.0.0 e con un TTL uguale a 0. in seguito a questo invio la CPU si intasa rallentando così le operazioni di routing della macchina.

2 attacco DoS: i prodotti della serie SSR 800 con firmware 2.x hanno un bug per cui sono vulnerabili ad attacchi di tipo denial of service portato sottoforma di invio ripetuto di richieste ARP. Il risultato è anche in questo caso un rallentamento dei processi di routing.

>> Cisco

È il più importante produttore mondiale nel campo dei router e delle piattaforme di interconnessioni fra reti, con un'offerta che spazia dalla famiglia alla grande azienda. All'indirizzo www.cisco.com sono reperibili tutte le informazioni utili sui vari prodotti dell'offerta.
I rischi documentati per questa marca sono:

1 attacchi DoS: portano ad un blocco di sistema o ad un accesso non autorizzato al loro interno. I prodotti potenzialmente vulnerabili a questi attacchi sono: router 2500 - 3660 — 4000 — 7100 — 7200 — 7500, i server di accesso AS5200 — AS5300 — AS5800, il system controller SC3640

e gli access path LS-3 — TS-3 — VS-3. un invio di pacchetti alla porta syslog (514 UDP) provoca il blocco di alcuni sistemi, inoltre una scansione ENVIRON può, in determinate circostanze, bloccare il sistema. L'attacco che più spesso viene portato è quello di tipo TCP SYN contro porte diagnostiche della macchina. E' un attacco noto col nome di Pepsi ed il listato, pepsi.c, può essere rintracciato in rete.

2 **IOS password cracker**: su alcuni modelli, utilizzando un listato tipo crackIOS.pl, si può riuscire a raccare le password di sistema garantendosi così l'accesso alla configurazione.

3 **attacco UDP scan**: alcuni router con sistema operativo 12.0 possono essere bloccati da una scansione UDP sulla porta 514. i modelli interessati sono quelli che adottano il software IOS 4000 (C4000-IK2S-M) versione IOS 12.0 ed il software IOS 2500 con versione 12.0

>> Intel

Da tempo Intell non fa solo microprocessori, e da poco è entrata anche nel mercato dei router, con offerte rivolte soprattutto alla media utenza. Il sito di riferimento è www.intel.com.

I rischi documentati per questa famiglia di prodotti sono:

1 **attacchi DoS**: scansioni remote effettuate con pacchetti ICMP di grandi dimensioni oppure con pacchetti ICMP frammentati possono portare a un accesso non autorizzato al sistema oppure ad un suo blocco. La serie di prodotti colpiti sono i router Intel Express. Su internet è reperibile il listato isic.h che contiene anche un frammento di codice adatto allo sfruttamento di tale bug.

C4TAR4TTA

IDENTIFICATION ORDER NO.
16 Gennaio 2003

WANTED

DIVISION OF INVESTIGATION
H.J. DEPARTMENT OF NET
CERNUSCO S.N., MI

Fingerprint Classification
16 0 5 U 001 20
I 17 U 001

KIDNAPING

NOME: SIRCAM

Alias: W32/SirCam@mm, Backdoor.SirCam, I-Worm.Sircam.a, WORM_SIRCAM.A, W32/Sircam-A, W32/Sircam, Win32.Sircam.137216, W32/Sircam.worm@mm, Win32.HLLW.SirCam

Sistemi a rischio: Windows 95, Windows 98, Windows Me

Sistemi immuni: Windows 3.x, Windows NT, Windows 2000, Windows XP, Macintosh, Unix, Linux

Nonostante questo worm sia stato scoperto oltre un anno fa, il 24 Novembre 2001 per la precisione, Badtrans continua a colpire i sistemi meno protetti e vulnerabili, anche se negli ultimi mesi si è assistito ad un enorme calo della sua diffusione che ha portato la Symantec ad abbassare la sua soglia di pericolosità da 4 a 3, dato l'aumento della sicurezza e la presenza costante di un antivirus installato sui computer.

DETTAGLI TECNICI

Quando Badtran viene eseguito su un computer provvede subito a copiare sè stesso nella cartella di sistema, che varia a seconda delle varie versioni di Windows, come file Kernel32.exe. Subito si registra come un processo di sistema, crea nella cartella di sistema il file log Cp_25389.nls e disabilita il file Kdll.dll, che contiene il codice per decifrare i log delle operazioni compiute sulla macchina. Badtrans ha l'originale funzione di utilizzare un timer per esaminare ogni secondo le finestre aperte e controllare se i titoli di queste iniziano con le parole log, pas, rem, con, ter o net. Queste lettere infatti formano le inziali delle parole logon, password, remote, connection, terminal e network ma nella lista delle lettere da controllare ci sono anche termini tradotti in altre lingue. Se una di queste parole viene trovata nel titolo di una finestra, allora viene attivato un key logging per 60 secondi che registra tutte le operazioni effettuate. Ogni 30 secondi, il file log e le password rilevate vengono inviate ad uno di questi indirizzi o ad altri che non sono più operativi, come:

ZVDOHYIK@yahoo.co
udtzqccc@yahoo.com
DTCELACB@yahoo.com
I1MCH2TH@yahoo.com
WPADJQ12@yahoo.com
smr@eurosport.com
bgnd2@canada.com
muwripa@fairesuivre.com
eccles@ballsy.net
S_Mentis@mail-x-change.com
YJPFJTGZ@excite.com
JGQZCD@excite.com
XHZJ3@excite.com
OZUNYLRL@excite.com
tsnlqd@excite.com
cxkawog@krovatka.net
ssdn@myrealbox.com

Dopo 20 secondi il worm disattiva queste operazioni se sono andate a buon fine altrimenti comincia la routine da capo.

DIFFUSIONE

Il worm arriva come un'E-mail con un allegato composto dal nome viariabile e da una combinazione di due estensioni. Se sul computer infetto è presente un supporto RAS, il worm attende una connessione RAS attiva per poi cercare indirizzi E-Mail nei file .ht* e .asp contenuti in determinate cartelle. Se vengono trovati indirizzi in questi file, Badtrans invia loro un'E-Mail tramite il server SMTP della vittima. Nel caso questo server non sia disponibile, il worm utilizza una propria lista di server SMTP. Il nome dell'allegato all'E-Mail infetta sarà uno dei seguenti: Pics, images, README, New_Napster_Site, news_doc, HAMSTER, YOU_are_FAT!, stuff, SETUP, Card, Me_nude, Sorry_about_yesterday, info, docs, Humor, fun.
In tutti i casi, MAPI sarà anche usato per trovare E-Mail non lette, contenute

nel proprio programma di posta elettronica, alle quali rispondere: in questo caso i soggetti dell'E-Mail saranno variabili ma inizieranno tutti con "Re:", tipico delle E-Mail di risposta.
Il worm utilizza una doppia estensione per camuffare gli allegati infetti alle E-Mail, in modo da aumentare la sua possibilità di propagazione: la prima estensione varia tra doc, mp3 e zip, che offrono all'utente meno esperto un'apparente tranquillità, mentre la seconda estensione sarà pif o scr. È proprio per questo consigliabile a tutti gli utenti Windows deselezionare l'opzione del proprio sistema operativo di nascondere le estensioni per i tipi di file conosciuti perché, non solo in questo caso, è facile farsi ingannare da una doppia estensione che nasconde un eseguibile pronto a danneggiare la nostra macchina. Il campo del mittente contiene un altro indirizzo tra quelli trovati sul computer infetto, ma potrebbe essere anche uno preso a caso da una lista contenuta nel worm proprio allo scopo di rendere vani i tentativi di risalire al vero mittente. Il worm scrive gli indirizzi E-Mail trovati nel file Protocol.dll, localizzato nella cartella di sistema, per evitare l'invio multiplo di E-Mail infette allo stesso indirizzo. Dopo aver inviato l'E-Mail, il worm aggiunge il valore Kernel32 e kernel32.exe alla chiave di registro

```
HKEY_LOCAL_MACHINE\Software\
Microsoft\Windows\CurrentVer
sion\RunOnce
```

che permette al worm di eseguirsi automaticamente al prossimo avvio di Windows e a tutti gli altri che seguiranno. Come per BugBear, anche Badtrans inserisce i valori nella chiave RunOnce e non Run: la differenza sostanziale tra le due è che la prima esegue i file a cui sono diretti i valori al suo interno al primo riavvio di Windows per poi eliminarlo mentre la seconda esegue il file a ogni avvio. Questo exploit serve a rendere difficile la localizzazione e l'annullamento di questa procedura dato che, con l'avvio del file al primo riavvio di Windows, viene aggiunto di nuovo lo stesso alla chiave RunOnce in modo da formare una catena difficile da scovare e da spezzare.

All'indirizzo www.rav.ro/ravmsstats si possono trovare interessanti statistiche sulla diffusione dei virus, aggiornate in tempo reale.

RACCOMANDAZIONI

Come per ogni worm, ci sono alcune buone norme di base da applicare per ottenere una discreta sicurezza e un minimo di tranquillità mentre si naviga su Internet:
- Eliminare o disinstallare tutte le applicazioni e i servizi non necessari per tenere sotto controllo facilmente il proprio sistema.
- Mantenere alto il livello e la frequenza degli aggiornamenti dei sofware di sicurezza in modo da non trovarsi impreparati o sprovvisti in caso di attacco.
- Adottare un comportamento di vigilanza per quanto riguarda le proprie password: è consigliabile utilizzare parole complesse o combinazioni complicate per diminuire la facilità con cui possono essere portati a termine gli attacchi e per limitare i danni nel caso che si venga comunque infettati.
- Configurare il proprio account E-Mail con un filtro che, come per lo spam, possa rimuovere le E-Mail che contengono allegati con estensioni tipiche dei virus, come exe, scr, vbs, bat e pif.
- Nel caso ci si accorga troppo tardi del virus contenuto in un file ed il sistema è già stato infettato è caldamente consigliato isolare velocemente la macchina infetta da network o altri computer in rete per evitare la diffusione incontrollata del worm.

RIMOZIONE

Come di consuetudine la Symantec ha realizzato un software per la rimozione del worm che potete trovare all'indirizzo http://securityresponse.symantec.com/avcenter/venc/data/w32.badtrans.b@mm.removal.tool.html. Allo stesso modo, lo strumento di Trend Micro per rimuovere Badtrans è disponibile all'indirizzo Web www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_BADTRANS.A
Esiste anche una procedura manuale di rimozione del worm, nel caso non si riuscisse a scaricare in file per qualche ragione, ma è molto lunga e complessa da eseguire e inoltre varia per ogni versione di Windows; per chi ne avesse comunque bisogno la si può trovare sul sito Symantec, nella pagina relativa a Badtrans.

{RoSwEIL}

ALCUNI DEI RISCHI CONNESSI ALL'UTILIZZO DI NETBIOS

IL PERICOLO DELLA CONDIVISIONE

Sempre più spesso la letteratura specializzata presenta articoli su come realizzare una Lan interna. Ciò, vista anche la mancanza di informazione della maggioranza degli utenti, che spesso condividono tra loro i dischi fissi dei PC, crea notevoli problemi di sicurezza.

1

Questo articolo serve per proteggere se stessi. **Non utilizzate questo testo per fare ca%%ate in giro**. Usate quanto indicato in questo testo solo per proteggere il vostro PC da visite indesiderate.
Tutti i discorsi che faremo valgono esclusivamente per i sistemi operativi Microsoft della generazione Windows 9x (Me compreso).

>> SMB, NETBios e NETBeui

SMB è un protocollo creato da IBM a metà degli anni Ottanta e successivamente adottato e implementato da Microsoft. Il funzionamento di questo protocollo, che opera a livello applicazione e presentazione, è sia di tipo Server (consente l'accesso a cartelle di file e stampanti da remoto) che di tipo client (consente di vedere sul proprio Pc le risorse condivise da un qualsiasi utente in rete).

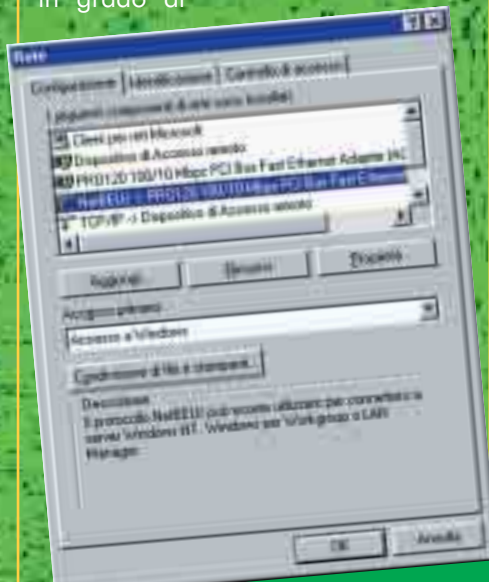
?

SMB Server Message Blocks. Il sistema usato su DOS/Windows per comunicare agli altri computer della rete le condivisioni disponibili.

In pratica, **SMB ha lo scopo di rendere visibili e utilizzabili da remoto, cartelle, file e stampanti**. Su tali risorse è possibile eseguire tutte le normali operazioni che si eseguono su cartelle e file presenti sul nostro Pc (lettura, scrittura, creazione, cancellazione eccetera). Per rendere le cose più semplici, Microsoft ha dotato SMB di un prodigioso componente chiamato Redirector che ci consente di disporre delle risorse remote , ovviamente condivise, come se fossero delle risorse locali.

?

NetBIOS Network Basic Input/Output System. L'API che consente di collegare i messaggi SMB alle funzionalità di sistema.

Grazie al redirector è cioè possibile vedere una cartella condivisa da un pc remoto come se fosse una cartella presente sul proprio Pc Per quanto concerne la sicurezza, il protocollo SMB è in grado di gestire due tipi di sicurezza: a livello condivisione e a livello utente.

Da Preferenze di Rete si possono aggiungere, rimuovere o configurare i supporti per i vari protocolli. Se non si utilizza la condivisione di file e stampanti, conviene rimuovere NetBEUI.

Nella sicurezza a livello condivisione viene richiesta una password per ogni elemento condiviso. Inserita questa password è possibile utilizzare le risorse poste all'interno della condivisone. Le operazioni che un utente potrà compiere sono fissate da chi condivide la risorsa.
In soldoni: supponiamo di aver condiviso in lettura: il disco c:\ con una password, la cartella c:\documenti con un'altra pass., In questo caso chi è in possesso della pass di accesso al disco c:\ può anche accedere alla cartella documenti in quanto documenti è interna alla condivisione c:\, viceversa chi possiede la pass di accesso alla cartella c:\documenti potrà accedere alle sole cartelle e/o file interni alla cartella documenti stessi.
Questo tipo di protezione soffre di un baco nell'autenticazione delle password scoperto da NSFOCUS Security Team il 18.09.00 e sfruttato dell'exploit Pqwak.exe di shiane hird 2000
Nel caso dell'autenticazione a livello utente, per accedere alle risorse condivise, l'utente remoto deve autenticarsi tramite la combinazione classica USER, PASSWORD. In questo caso le operazioni che questo utente potrà compiere sono legate ai privilegi che l'utente possiede all'interno della Lan. In soldoni, in queste reti deve esistere un server NT ove risiede il file delle autorizzazioni.

>> I livelli sottostanti

Per quanto finora detto SMB è un protocollo funzionante a livello Applicazione/presentazione per il tra-

sporto dei pacchetti e quindi per la comunicazione , in rete, si avrà bisogno di altri protocolli (protocolli che operino a livello Sessione, Trasporto, Network, Data link e Fisico).
Microsoft ha scelto due possibili protocolli (in seguito vedremo il perché):

- **NETBEUI**
- **TCP/IP**

Come saprete, TCP/IP lavora a livello trasporto network. Il collegamento quindi tra SMB e TCP/IP, e ovviamente anche attraverso Netbeuì, avviene attraverso un API che funzioni a livello sessione chiamata NETBIOS (nel netbeui il netbios è un componente fondamentale).
Le comunicazioni tra SMB e il livello inferiore (netbios) avvengono tramite strutture di dati chiamate NCB: Network Control Bloc.
Ricapitolando:
SMB è usato da Windows 3.x, 9.x, Nt e OS/2 per permettere l'accesso e la condivisione di cartelle, file e stampanti remote.
NETBIOS è un API che funziona a livello Sessione e che ha il compito di unire l'SMB con i protocolli necessari per l'instradamento dei pacchetti come TCP, IP, IPX...
NETBEUI è un protocollo, contenente l'API netbios, per il trasporto dei pacchetti che ha la possibilità di dialogare direttamente con l'SMB.

NetBEUI NetBIOS extended User Interface. Versione migliorata del protocollo NetBIOS, per l'implementazione di reti locali.

Ricordiamo che Netbeui non è altro che un'implementazione di netbios in grado di compiere il trasporto dei dati.
Netbios nasce circa negli anni 80 e ha come obiettivo principale quello di rendere più umane le LAN. In pratica si tenta di eliminare i complessi indirizzi numerici e di sostituirli con nomi.

>> Come funziona

Quando un client vuole registrarsi in una rete, questi manda un messaggio dì tipo broadcast (uno a tutti) in cui viene indicato il proprio nome. Se questo nome è già esistente, allora accadrà che il client in possesso dei nome comunicherà tramite connessione di tipo PPP (point to point) che il nome che si vuole utilizzare è già esistente e quindi un diniego alla connessione in rete.
Se il client che sta tentando la registrazione non riceve risposta allora questi diventa punto attivo della rete stessa.

NBT NetBIOS over TCP/IP. Estende anche su reti Internet le funzionalità di NetBIOS, che altrimenti sarebbero limitate alla sola sottorete.

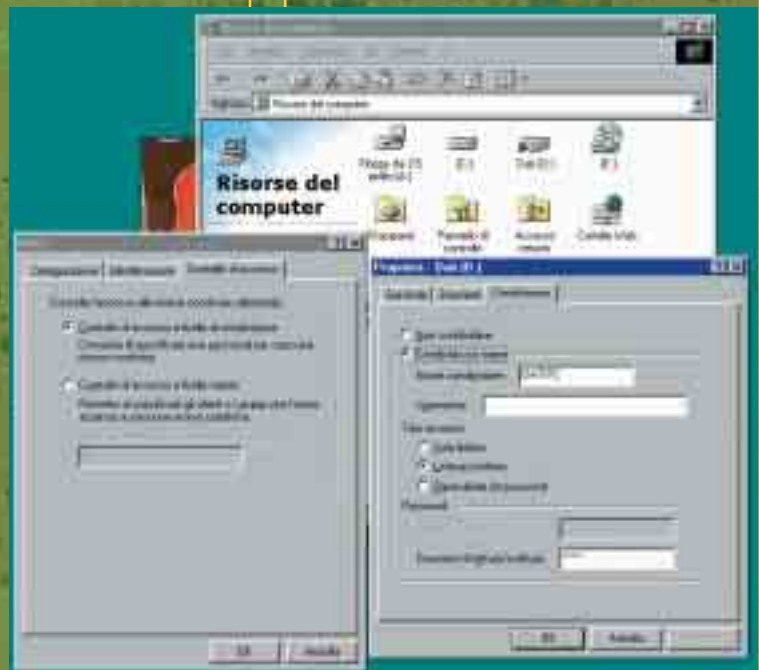
1. Le comunicazioni tra due client o nodi invece avvengono nel seguente modo:
2. Il client1 invia un broadcast, contenente il nome del client da contattare, a tutta la rete.
3. Il client2, se presente, risponderà al clienti tramite un messaggio punto a punto (PPP).

A questo punto si stabilisce una connessione di tipo PPP tra i due client.

Le comunicazioni, in una rete che utilizza il netbios, possono essere di tre tipi:

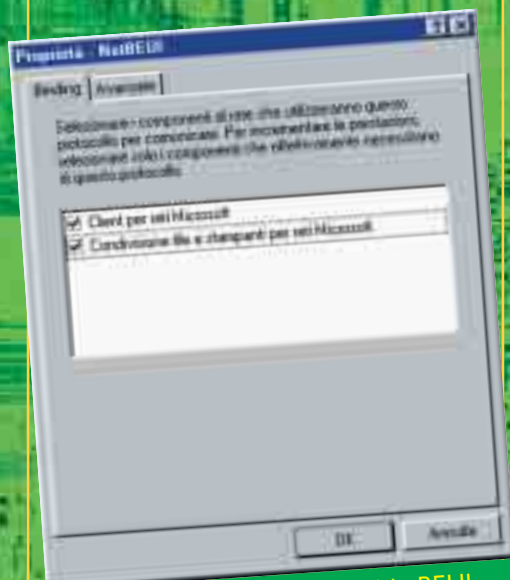
- **Sessioni:** si usano per scambiare con un altro client/nodo rilevanti quantità di dati.
- **Datagrammi:** servono per inviare a più nodi di un gruppo messaggi di modeste dimensioni massime di 512 byte.
- **Broadcast:** messaggi a tutti i nodi presenti di modeste dimensioni.

I nomi utilizzati da Netbios sono composti da 16 caratteri alfanumerici (la $ finale è utilizzata per nascondere le condivisioni. Per esempio, la cartella condivisa con nome documenti$, pur esistendo ed essendo condivisa, non sarà visibile dentro alle Risorse di Rete degli altri utenti.

I nomi possono essere Unici (Individuano un client o un determinato servizio offerto) o Gruppi (identificano il "gruppo" a cui il client o la risorsa appartiene).
Il Netbeui non utilizza porte, quindi per indicare se il nome unico è un servizio o un client viene utilizzato un carattere dei sedici a disposizione.
Questo carattere, noto come suffisso, è indicato in esadecimale. Per esempio il nome con a fianco il suffisso 46 indica che è attivo l'SMS client remote trasfert. Il suffisso 20 invece indica che il client ha abilitato la possibilità di condivisione delle risorse.
Per la tabella completa suffissi / servizi si rimanda al sito http://support.microsoft.com/default.aspx?scid=kb;en-us;163409.
Per vedere la tabella dei servizi offerti

In alto, si può vedere come appare un disco condiviso in Risorse del Computer (Dati, D:). A sinistra, la finestra dove si imposta il metodo di autenticazione, e a destra la finestra per impostare la password di protezione.

in una rete basta utilizzare il comando: nbstat a nome_client (o servizio). Ultima cosa utile da sapere è che, per

LMHOST Si tratta di un file che risiede nella cartella c:\windows\. Se non è mai stato utilizzato ha estensione .sam (sample). Questo file nasce per diminuire le richieste broadcast. Al suo interno vengono indicati nomi e indirizzi. Quando questi sono accompagnati dal suffisso #PRE, allora vengono precaricati nella cache.

evitare che ogni client debba contenere una copia nome nodo / risorsa condivisa, in genere viene elet-

Le proprietà del protocollo NetBEUI; volendo, è possibile selezionare soli il Client, se non si devono condividre risorse della propria macchina.

to tra tutti i nodi un browser master a cui viene affidata la lista. In reti miste (Windows 9x, NT, unix...) la lista viene affidata a sistemi di classe superiore NT o Linux con Samba. In reti di soli windows 9x, si può scegliere il browser master selezionando: Pannello di controllo >Rete >Condivisione file e stampanti > Browser master >Attivato.

>> Limiti e problemi di Netbeui

Come già detto, per le comunicazioni, il protocollo utilizza in maniera massiccia il broadcast, e ciò comporta l'impossibilità di comunicazione tra due reti connesse attraverso router, un degrado di qualità delle Lan estese, la difficoltà (o l'impossibilità) di avere nomi unici nelle Wan, e l'impossibilità di effettuare un routing, ovvero di conoscere la posizione del nodo al quale ci vogliamo collegare.

Dato il crescente interesse degli utenti a Internet, Microsoft ha deciso di manipolare il netbios, creando NBT.

1. NBT è un ibrido in cui il Netbios supporta i nomi, mentre TCP/IP supporta invece gli indirizzi numerici.
2. Un client Windows, in questo tipo di rete, per effettuare una connessione con un altro client procede nel seguente modo:

Consulta una cache interna HKEY CURRENT_USER >recent.

3. Interroga se presente nella rete un server wins (un server wins è l'equivalente di un server DNS, ovvero consente di associare a un nome un indirizzo IP e viceversa).
4. Fa un broadcast.

Consulta un file interno LMHOST.

Combinando nomi e indirizzi IP, NBT consente di superare i limiti dei netbeui, ma al contempo mette a rischio tutte le condivisioni presenti in una Lan.0

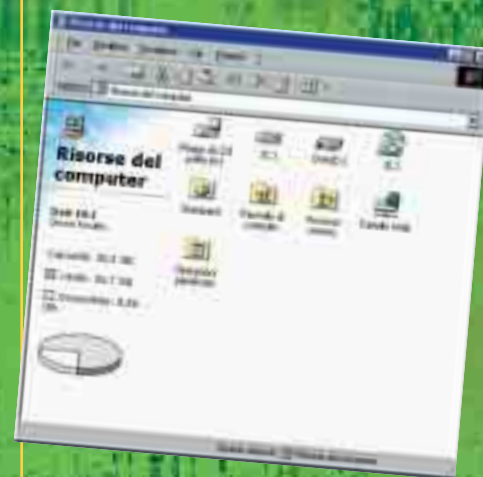
Affinché le comunicazioni possano avvenire regolarmente con TCP/IP, è necessario che siano aperte le porte per i tre possibili tipi di comunicazione usati dal netbios. Queste porte sono:

- **137:** Risoluzione dei nomi Netbios (UDP)
- **138, 139:** datagrammi (UDP)
- **139:** sessioni (TCP).

>> La questione della sicurezza

Vediamo come un malintenzionato potrebbe applicare quanto finora visto, e cercare di violare il nostro computer.

Ricerca della vittima

Chi usa NBT ha sicuramente le porte 137, 138, 139 aperte. (Attenti che a causa di un baco di Windows chi installa TCP/IP, automaticamente installa anche il Netbios e quindi avrà aperte le fatidiche porte 137,138,139; se non ci credete, date il comando dalla shell del dos netstat a). Con uno scanner impostato sulla porta 139, trovare un computer con Netbios attivo è solo questione di (poco) tempo.

Verifica delle vittima

Dopo avere individuato la sua vittima, il cracker andrà a vedere quali cartelle o elementi sono condivisi. Dalla shell del Dos gli basterà fare nbtstat a xxx.xxx.xxx.xxx, oppure nbtstat a nome. Se tra i suffissi c'è il 20, la vittima ha attive le condivisioni di cartelle file e stampanti.

Inserimento in LMHOST

L'attacker inserirà quindi la vittima nella sua "fan". Per far ciò, sfrutterà il file LMHOST e il suffisso #PRE. Ossia editerà il file LMNOST, inserendo all'interno la voce:

```
xxx.xxx.xxx.xxx <tab> <nome
macchina> <tab> #pre
```

Salverà il file senza suffissi. Il nome macchina lo avrà ricavato da nbtstat A xxx.xxx.xxx.xxx (il primo nome che compare nella lista). A questo punto darà il comando nbtstat R (in pratica inserirà il contenuto di LMHST nella cache).

Livelli OSI	NetBEUI	NetBIOS over TCP/IP	TCP/IP
Applicazione	SMB	SMB	Telnet, Ftp, SMTP...
Presentazione			
Sessione	NetBEUI	NetBIOS	
Trasporto		TCP, UDP	TCP, UDP
Network		IP ICMP	IP ICMP
Data Link	Non dipende dai protocolli superiori		
Livello Fisico			

Come i vari protocolli sono distribuiti tra i vari livelli della cosiddetta "Pila OSI", che schematizza la struttura di una rete.

Elenco delle risorse
A questo punto, cercherà di capire se la vittima ha solo la possibilità di condividere risorse, o se ha le
ha effettivamente effettivamente condivise: il comando da dare è

net view \\<nome computer>

Utilizzo delle risorse condivise
Per far ciò userà redirector. Utilizzerà Internet Explorer inserendo l'indirizzo

xxx.xxx.xxx.xxx/<cartella condivisa>

oppure dal menu Start>Esegui

\\ xxx.xxx.xxx.xxx/<cartella condivisa>

Oppure ancora, dal menu Strumenti > Connetti unità di rete > xxx.xxx.xxx.xxx/cartella condivisa.

>> Un altro metodo

Trovata la sua vittima e constatato che questi ha attiva la condivisione delle risorse (suffisso 20), l'attaccante potrebbe sfruttare un baco di Windows che consente la connessione nulla alle cartelle nascoste (IPC$, C$ ADMIN$). In pratica, in caso di protezione a livello di condivisione userà il seguente comando:

```
net use
\\xxx.xxx.xxx.xxx\IPC$
```

Se la protezione avvenisse a livello utente, utilizzerà il comando

```
net use \\xxx.xxx.xxx.\IPC$

"/<utente>:"
```

A questo punto, con il comando:

```
net view \\xxx.xxx.xxx\
```

otterrà l'elenco delle cartelle condivise.

>> Come difendersi

Innanzi tutto, conviene disattivare la possibilità di connessione "nulla". Bisogna operare sul registro di configurazione, precisamente alla chiave:

```
HKEY_LOCAL
MACHINE\System\CurrentContr
olSet\ControI1LSA
```

e aggiungere

```
value name:
RestrictAnonymous data type
: REG_DWORD, value 1
```

Questo vale solo per windows NT.

Oltre ovviamente a **scegliere password lunghe e non facilmente individuabili** (sequenze casuali di lettere e numeri, per esempio), possiamo anche fare qualcosa in più per cercare di accorgerci di un tentativo di intrusione.
Per esempio, si può **usare un programma come NetAlarm** (www.thomasmathiesen.com/html/software/netalert2.html), che verifica costantemente l'attività delle condivisioni.
Volendo, si può lasciare una condivisione aperta senza password (e senza niente di importante dentro!) da **esporre come esca per il lamerone di turno**. Probabilmente ci si tufferà, facendo scattare l'allarme di NetAlert e **permettendoci di prendere le contromisure del caso** (filtrare il suo IP dal firewall, per esempio).
Qualcuno si spinge più in la, e **nella "finta condivisione" infila programmi con backdoor e trojan, camuffati da software innocui o persino da documenti dal nome appetitoso** (carta-di-credito.txt.exe... c'è sempre qualcuno che ci casca). Chi tentasse di aprire quel file, lo aprirebbe sul proprio computer, infettandosi. A rigore, in questo caso non si sta distribuendo un software dannoso (è il malintenzionato che viene a prendersel dal nostro computer, senza che noi lo abbiamo autorizzato). **In realtà la pratica non è comunque molto pulita...**
Se la condivisione non ci interessa, possiamo disabilitarla dalle preferenze di Rete e, per soprammercato, **chiudere le porte 139, 138 e 137 con un firewall**.
Per navigare in Internet, infatti, l'unico protocollo necessario è il TCP/IP, e **se non avete una rete di più computer, non è necessario tenere attivi i protocolli a essa dedicati**.
Se invece una rete c'è, si possono separare le zone interna ed esterna. Invece che NBT, la Lan può tranquillamente utilizzare il NETBEUI, che non apre porte di comunicazione. I binding delle schede di rete devono essere solo verso i protocolli interni NETBEUI, e i binding quelli dei Modem solo su TCP/IP. Ma di questo argomento ci occuperemo in un altro articolo.

BartMan